# Cisco ME 2400 Ethernet Access Switch Command Reference

Cisco IOS Release 12.2(44)SE
January 2008

**Americas Headquarters**
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Text Part Number: OL-9643-03

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CCVP, the Cisco logo, and Welcome to the Human Network are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networkers, Networking Academy, Network Registrar, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0711R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

*Cisco ME 2400 Ethernet Access Switch Command Reference*
© 2006-2008 Cisco Systems, Inc. All rights reserved.

# CONTENTS


**Preface** xv

Audience xv

Purpose xv

Conventions xvi

Related Publications xvi

Obtaining Documentation and Submitting a Service Request xvii

CHAPTER 1 **Using the Command-Line Interface** 1-1

CLI Command Modes 1-1

User EXEC Mode 1-2

Privileged EXEC Mode 1-3

Global Configuration Mode 1-3

Interface Configuration Mode 1-4

VLAN Configuration Mode 1-4

Line Configuration Mode 1-4

CHAPTER 2 **Cisco ME 2400 Ethernet Access Switch Cisco IOS Commands** 2-1

aaa accounting dot1x 2-1

aaa authentication dot1x 2-3

action 2-5

archive download-sw 2-7

archive tar 2-10

archive upload-sw 2-13

bandwidth 2-15

boot boothlpr 2-18

boot config-file 2-19

boot enable-break 2-20

boot helper 2-21

boot helper-config-file 2-22
boot manual 2-23
boot private-config-file 2-24
boot system 2-25
channel-group 2-26
channel-protocol 2-30
class 2-32
class-map 2-34
clear ip dhcp snooping 2-36
clear lacp 2-38
clear mac address-table 2-39
clear pagp 2-40
clear policer cpu uni-eni counters 2-41
clear port-security 2-42
clear spanning-tree counters 2-44
clear spanning-tree detected-protocols 2-45
clear vmps statistics 2-47
conform-action 2-48
define interface-range 2-50
delete 2-52
deny (MAC access-list configuration) 2-53
dot1x default 2-56
dot1x host-mode 2-57
dot1x initialize 2-58
dot1x max-reauth-req 2-59
dot1x max-req 2-60
dot1x port-control 2-61
dot1x re-authenticate 2-63
dot1x reauthentication 2-64
dot1x system-auth-control 2-65
dot1x test eapol-capable 2-66
dot1x test timeout 2-67
dot1x timeout 2-68

duplex 2-70
errdisable detect cause 2-72
errdisable detect cause small-frame 2-74
errdisable recovery cause small-frame 2-76
errdisable recovery 2-77
exceed-action 2-79
flowcontrol 2-81
interface port-channel 2-83
interface range 2-85
interface vlan 2-88
ip access-group 2-89
ip address 2-91
ip dhcp snooping 2-93
ip dhcp snooping binding 2-94
ip dhcp snooping database 2-96
ip dhcp snooping information option 2-98
ip dhcp snooping information option allowed-untrusted 2-100
ip dhcp snooping information option format remote-id 2-102
ip dhcp snooping limit rate 2-103
ip dhcp snooping trust 2-104
ip dhcp snooping verify mac-address 2-105
ip dhcp snooping vlan 2-106
ip dhcp snooping vlan information option format-type circuit-id string 2-107
ip igmp filter 2-109
ip igmp max-groups 2-111
ip igmp profile 2-113
ip igmp snooping 2-115
ip igmp snooping last-member-query-interval 2-117
ip igmp snooping querier 2-119
ip igmp snooping report-suppression 2-121
ip igmp snooping tcn 2-123
ip igmp snooping tcn flood 2-124
ip igmp snooping vlan immediate-leave 2-125

ip igmp snooping vlan mrouter **2-126**
ip igmp snooping vlan static **2-128**
ip ssh **2-130**
lacp port-priority **2-132**
lacp system-priority **2-134**
logging event **2-136**
logging file **2-137**
mac access-group **2-139**
mac access-list extended **2-141**
mac address-table aging-time **2-143**
mac address-table notification **2-144**
mac address-table static **2-146**
mac address-table static drop **2-147**
macro apply **2-149**
macro description **2-151**
macro global **2-152**
macro global description **2-154**
macro name **2-155**
match (access-map configuration) **2-157**
match access-group **2-159**
match cos **2-160**
match ip dscp **2-161**
match ip precedence **2-163**
match qos-group **2-165**
mdix auto **2-167**
monitor session **2-169**
mvr (global configuration) **2-174**
mvr (interface configuration) **2-177**
pagp learn-method **2-180**
pagp port-priority **2-182**
permit (MAC access-list configuration) **2-184**
police **2-187**
police aggregate (policy-map class configuration) **2-191**

policer aggregate (global configuration) **2-193**
policer cpu uni **2-196**
policy-map **2-197**
port-channel load-balance **2-200**
port-type **2-202**
priority **2-204**
private-vlan **2-207**
queue-limit **2-210**
remote-span **2-213**
renew ip dhcp snooping database **2-215**
rmon collection stats **2-217**
service password-recovery **2-218**
service-policy (interface configuration) **2-220**
service-policy (policy-map class configuration) **2-222**
set cos **2-224**
set dscp **2-226**
set precedence **2-228**
set qos-group **2-230**
setup **2-232**
shape average **2-235**
show access-lists **2-237**
show archive status **2-240**
show boot **2-241**
show cable-diagnostics tdr **2-243**
show class-map **2-245**
show controllers cpu-interface **2-246**
show controllers ethernet-controller **2-248**
show controllers tcam **2-255**
show controllers utilization **2-257**
show dot1x **2-259**
show env **2-262**
show errdisable detect **2-263**
show errdisable flap-values **2-265**

show errdisable recovery 2-267
show etherchannel 2-269
show flowcontrol 2-272
show idprom 2-274
show interfaces 2-276
show interfaces counters 2-284
show inventory 2-286
show ip dhcp snooping 2-288
show ip dhcp snooping binding 2-289
show ip dhcp snooping database 2-291
show ip dhcp snooping statistics 2-293
show ip igmp profile 2-296
show ip igmp snooping 2-297
show ip igmp snooping groups 2-299
show ip igmp snooping mrouter 2-301
show ip igmp snooping querier 2-303
show lacp 2-305
show mac access-group 2-309
show mac address-table 2-311
show mac address-table address 2-313
show mac address-table aging-time 2-315
show mac address-table count 2-317
show mac address-table dynamic 2-319
show mac address-table interface 2-321
show mac address-table notification 2-323
show mac address-table static 2-325
show mac address-table vlan 2-327
show monitor 2-329
show mvr 2-331
show mvr interface 2-333
show mvr members 2-335
show pagp 2-337
show parser macro 2-339

show policer aggregate 2-341
show policer cpu uni-eni 2-342
show policy-map 2-344
show port-security 2-348
show port-type 2-351
show sdm prefer 2-353
show spanning-tree 2-354
show storm-control 2-360
show system mtu 2-362
show table-map 2-363
show udld 2-365
show version 2-367
show vlan 2-369
show vlan access-map 2-374
show vlan filter 2-375
show vmps 2-377
shutdown 2-379
shutdown vlan 2-380
small-frame violation rate 2-381
snmp-server enable traps 2-383
snmp-server host 2-386
snmp trap mac-notification 2-390
spanning-tree 2-392
spanning-tree bpdufilter 2-394
spanning-tree bpduguard 2-396
spanning-tree cost 2-398
spanning-tree etherchannel guard misconfig 2-400
spanning-tree extend system-id 2-402
spanning-tree guard 2-404
spanning-tree link-type 2-406
spanning-tree loopguard default 2-408
spanning-tree mode 2-410
spanning-tree mst configuration 2-412

spanning-tree mst cost 2-414
spanning-tree mst forward-time 2-416
spanning-tree mst hello-time 2-417
spanning-tree mst max-age 2-419
spanning-tree mst max-hops 2-421
spanning-tree mst port-priority 2-423
spanning-tree mst pre-standard 2-425
spanning-tree mst priority 2-426
spanning-tree mst root 2-428
spanning-tree port-priority 2-430
spanning-tree portfast (global configuration) 2-432
spanning-tree portfast (interface configuration) 2-435
spanning-tree vlan 2-437
speed 2-440
storm-control 2-442
switchport 2-445
switchport access vlan 2-447
switchport block 2-449
switchport host 2-451
switchport mode 2-452
switchport mode private-vlan 2-454
switchport port-security 2-457
switchport port-security aging 2-461
switchport private-vlan 2-463
switchport protected 2-465
switchport trunk 2-467
system mtu 2-469
table-map 2-471
test cable-diagnostics tdr 2-473
traceroute mac 2-474
traceroute mac ip 2-477
udld 2-479
udld port 2-481

udld reset **2-483**
uni-vlan **2-484**
vlan **2-486**
vlan access-map **2-489**
vlan filter **2-491**
vmps reconfirm (privileged EXEC) **2-493**
vmps reconfirm (global configuration) **2-494**
vmps retry **2-495**
vmps server **2-496**

APPENDIX A

**Cisco ME 2400 Ethernet Access Switch Boot Loader Commands** **A-1**

boot **A-2**
cat **A-4**
copy **A-5**
delete **A-6**
dir **A-7**
flash_init **A-9**
format **A-10**
fsck **A-11**
help **A-12**
memory **A-13**
mkdir **A-14**
more **A-15**
rename **A-16**
reset **A-17**
rmdir **A-18**
set **A-19**
type **A-22**
unset **A-23**
version **A-25**

APPENDIX B

Cisco ME 2400 Ethernet Access Switch Debug Commands B-1

debug dot1x B-2
debug etherchannel B-3
debug interface B-4
debug ip igmp filter B-5
debug ip igmp max-groups B-6
debug ip igmp snooping B-7
debug lacp B-8
debug mac-notification B-9
debug matm B-10
debug monitor B-11
debug mvrdbg B-12
debug nvram B-13
debug pagp B-14
debug platform acl B-15
debug platform cpu-queues B-16
debug platform dot1x B-18
debug platform etherchannel B-19
debug platform forw-tcam B-20
debug platform ip dhcp B-21
debug platform ip igmp snooping B-22
debug platform led B-24
debug platform matm B-25
debug platform messaging application B-26
debug platform phy B-27
debug platform pm B-29
debug platform policer cpu uni-eni B-31
debug platform port-asic B-32
debug platform port-security B-33
debug platform qos-acl-tcam B-34
debug platform remote-commands B-35
debug platform resource-manager B-36
debug platform snmp B-37

debug platform span B-38
debug platform supervisor-asic B-39
debug platform sw-bridge B-40
debug platform tcam B-41
debug platform udld B-43
debug platform vlan B-44
debug pm B-45
debug port-security B-47
debug qos-manager B-48
debug spanning-tree B-49
debug spanning-tree bpdu B-51
debug spanning-tree bpdu-opt B-52
debug spanning-tree mstp B-53
debug spanning-tree switch B-55
debug sw-vlan B-57
debug sw-vlan ifs B-58
debug sw-vlan notification B-59
debug udld B-61
debug vqpc B-63

APPENDIX C

**Cisco ME 2400 Ethernet Access Switch Show Platform Commands** C-1

show platform acl C-2
show platform configuration C-3
show platform etherchannel C-4
show platform forward C-5
show platform ip igmp snooping C-7
show platform layer4op C-9
show platform mac-address-table C-10
show platform messaging C-11
show platform monitor C-12
show platform mvr table C-13
show platform pm C-14
show platform policer cpu C-16

show platform port-asic C-19
show platform port-security C-23
show platform qos C-24
show platform resource-manager C-27
show platform snmp counters C-29
show platform spanning-tree synchronization C-30
show platform stp-instance C-31
show platform tcam C-32
show platform vlan C-35

INDEX

# Preface

## Audience

This guide is for the networking professional using the Cisco IOS command-line interface (CLI) to manage the Cisco Metro Ethernet (ME) 2400 Series Ethernet Access switch, hereafter referred to as *the switch*. Before using this guide, you should have experience working with the Cisco IOS commands and the switch software features. You should also have experience working with the concepts and terminology of Ethernet and local area networking.

## Purpose

This guide provides the information you need about the Layer 2 commands that have been created or changed for use with the Cisco ME 2400 Ethernet Access switch. For information about the standard Cisco IOS Release 12.2 commands, see the Cisco IOS documentation set available from the Cisco.com home page by selecting **Service and Support > Technical Documents**. On the Cisco Product Documentation home page, select **Release 12.2** from the Cisco IOS Software drop-down list.

This guide does not provide procedures for configuring your switch. For detailed configuration procedures, see the software configuration guide for this release.

This guide does not describe system messages you might encounter. For more information, see the system message guide for this release.

For the latest documentation updates, see the release notes for this release.

# Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in **boldface** text.
- Arguments for which you supply values are in *italic*.
- Square brackets ([ ]) means optional elements.
- Braces ( ) group required choices, and vertical bars ( | ) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in `screen` font.
- Information you enter is in **`boldface screen`** font.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes, cautions, and warnings use these conventions and symbols:

**Note** Means *reader take note*. Notes contain helpful suggestions or references to materials not contained in this manual.

**Caution** Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

# Related Publications

These documents provide complete information about the switch and are available from this Cisco.com site:

http://www.cisco.com/en/US/products/ps6581/tsd_products_support_series_home.html

**Note** Before installing, configuring, or upgrading the switch, see these documents:

- For initial configuration information, see the "Configuring the Switch with the CLI-Based Setup Program" appendix in the hardware installation guide.
- For upgrading information, see the "Downloading Software" section in the release notes.

You can order printed copies of documents with a DOC-xxxxxx= number from the Cisco.com sites and from the telephone numbers listed in the URL referenced in the "Obtaining Documentation and Submitting a Service Request" section.

- *Release Notes for the Cisco ME 2400 Ethernet Access Switch for* (not orderable but available on Cisco.com)

- *Cisco ME 2400 Ethernet Access Switch Software Configuration Guide* (not orderable but available on Cisco.com)
- *Cisco ME 2400 Ethernet Access Switch Command Reference*(not orderable but available on Cisco.com)
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches System Message Guide* (not orderable but available on Cisco.com)
- *Cisco ME 2400 Ethernet Access Switch Hardware Installation Guide* (not orderable but available on Cisco.com)
- *Cisco ME 3400 and ME 2400 Ethernet Access Switches Getting Started Guide (*order number DOC-7817050=)
- *Regulatory Compliance and Safety Information for the Cisco ME 3400 and ME 2400 Ethernet Access Switches* (order number DOC-7817051)
- *Cisco Small Form-Factor Pluggable Modules Installation Notes* (order number DOC-7815160=)
- *Cisco CWDM GBIC and CWDM SFP Installation Note* (not orderable but available on Cisco.com)
- These compatibility matrix documents are available from this Cisco.com site:

http://www.cisco.com/en/US/products/hw/modules/ps5455/products_device_support_tables_list.html

  - *Cisco Gigabit Ethernet Transceiver Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Cisco 100-Megabit Ethernet SFP Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Cisco Small Form-Factor Pluggable Modules Compatibility Matrix* (not orderable but available on Cisco.com)
  - *Compatibility Matrix for 1000BASE-T Small Form-Factor Pluggable Modules* (not orderable but available on Cisco.com)

# Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

CHAPTER 1

# Using the Command-Line Interface

The Cisco Metro Ethernet (ME) 2400 Series Ethernet Access switch is supported by Cisco IOS software. This chapter describes how to use the switch command-line interface (CLI) to configure software features.

For a complete description command descriptions, see these sections:

- For the configuration and monitoring commands that support these features, see Chapter 2, "Cisco ME 2400 Ethernet Access Switch Cisco IOS Commands."
- For information on the boot loader commands, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."
- For information on the **debug** commands, see Appendix B, "Cisco ME 2400 Ethernet Access Switch Debug Commands."
- For information on the **show platform** commands, see Appendix C, "Cisco ME 2400 Ethernet Access Switch Show Platform Commands."
- For more information on Cisco IOS Release 12.2, see the *Cisco IOS Release 12.2 Command Summary*.

For task-oriented configuration steps, see the software configuration guide for this release.

In this document, IP refers to IP version 4 (IPv4).

## CLI Command Modes

This section describes the CLI command mode structure. Command modes support specific Cisco IOS commands. For example, the **interface** *interface-id* command only works when entered in global configuration mode.

These are the main command modes for the switch:

- User EXEC
- Privileged EXEC
- Global configuration
- Interface configuration
- VLAN configuration
- Line configuration

Table 1-1 lists the main command modes, how to access each mode, the prompt you see in that mode, and how to exit that mode. The prompts listed use the default name *Switch*.

***Table 1-1 Command Modes Summary***

| Command Mode | Access Method | Prompt | Exit or Access Next Mode |
|---|---|---|---|
| User EXEC | This is the first level of access.<br>(For the switch) Change terminal settings, perform basic tasks, and list system information. | `Switch>` | Enter the **logout** command.<br>To enter privileged EXEC mode, enter the **enable** command. |
| Privileged EXEC | From user EXEC mode, enter the **enable** command. | `Switch#` | To exit to user EXEC mode, enter the **disable** command.<br>To enter global configuration mode, enter the **configure** command. |
| Global configuration | From privileged EXEC mode, enter the **configure** command. | `Switch(config)#` | To exit to privileged EXEC mode, enter the **exit** or **end** command, or press **Ctrl-Z**.<br>To enter interface configuration mode, enter the **interface** configuration command. |
| Interface configuration | From global configuration mode, specify an interface by entering the **interface** command followed by an interface identification. | `Switch(config-if)#` | To exit to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.<br>To exit to global configuration mode, enter the **exit** command. |
| VLAN configuration | In global configuration mode, enter the **vlan** *vlan-id* command. | `Switch(config-vlan)#` | To exit to global configuration mode, enter the **exit** command.<br>To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. |
| Line configuration | From global configuration mode, specify a line by entering the **line** command. | `Switch(config-line)#` | To exit to global configuration mode, enter the **exit** command.<br>To return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**. |

# User EXEC Mode

After you access the device, you are automatically in user EXEC command mode. The EXEC commands available at the user level are a subset of those available at the privileged level. In general, use the user EXEC commands to temporarily change terminal settings, perform basic tests, and list system information.

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch> ?
```

# Privileged EXEC Mode

Because many of the privileged commands configure operating parameters, privileged access should be password-protected to prevent unauthorized use. The privileged command set includes those commands contained in user EXEC mode, as well as the **configure** privileged EXEC command through which you access the remaining command modes.

If your system administrator has set a password, you are prompted to enter it before being granted access to privileged EXEC mode. The password does not appear on the screen and is case sensitive.

The privileged EXEC mode prompt is the device name followed by the pound sign (#).

```
Switch#
```

Enter the **enable** command to access privileged EXEC mode:

```
Switch> enable
Switch#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch# ?
```

To return to user EXEC mode, enter the **disable** privileged EXEC command.

# Global Configuration Mode

Global configuration commands apply to features that affect the device as a whole. Use the **configure** privileged EXEC command to enter global configuration mode. The default is to enter commands from the management console.

When you enter the **configure** command, a message prompts you for the source of the configuration commands:

```
Switch# configure
Configuring from terminal, memory, or network [terminal]?
```

You can specify either the terminal or nonvolatile RAM (NVRAM) as the source of configuration commands.

This example shows you how to access global configuration mode:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config)# ?
```

To exit global configuration command mode and to return to privileged EXEC mode, enter the **end** or **exit** command, or press **Ctrl-Z**.

# Interface Configuration Mode

Interface configuration commands modify the operation of the interface. Interface configuration commands always follow a global configuration command, which defines the interface type.

Use the **interface** *interface-id* command to access interface configuration mode. The new prompt means interface configuration mode.

```
Switch(config-if)#
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-if)# ?
```

To exit interface configuration mode and to return to global configuration mode, enter the **exit** command. To exit interface configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

# VLAN Configuration Mode

Use this mode to configure normal-range VLANs (VLAN IDs 1 to 1005) or extended-range VLANs (VLAN IDs 1006 to 4094). The VLAN configuration is saved in the running configuration file, and you can save it to the switch startup configuration file by using the **copy running-config startup-config** privileged EXEC command. The configurations of VLAN IDs 1 to 1005 are saved in the VLAN database. The extended-range VLAN configurations are not saved in the VLAN database.

Enter the **vlan** *vlan-id* global configuration command to access VLAN configuration mode:

```
Switch(config)# vlan 2000
Switch(config-vlan)#
```

To display a comprehensive list of available commands, enter a question mark (**?**) at the prompt.

```
Switch(config-vlan)# ?
```

For extended-range VLANs, many characteristics are not configurable and must remain at the default setting.

To return to global configuration mode, enter **exit**; to return to privileged EXEC mode, enter **end**. All the commands except **shutdown** take effect when you exit config-vlan mode.

# Line Configuration Mode

Line configuration commands modify the operation of a terminal line. Line configuration commands always follow a line command, which defines a line number. Use these commands to change terminal parameter settings line-by-line or for a range of lines.

Use the **line vty** *line_number* [*ending_line_number*] command to enter line configuration mode. The new prompt means line configuration mode. The following example shows how to enter line configuration mode for virtual terminal line 7:

```
Switch(config)# line vty 0 7
```

The supported commands can vary depending on the version of software in use. To display a comprehensive list of commands, enter a question mark (**?**) at the prompt.

```
Switch(config-line)# ?
```

To exit line configuration mode and to return to global configuration mode, use the **exit** command. To exit line configuration mode and to return to privileged EXEC mode, enter the **end** command, or press **Ctrl-Z**.

CHAPTER 2

# Cisco ME 2400 Ethernet Access Switch Cisco IOS Commands

## aaa accounting dot1x

Use the **aaa accounting dot1x** global configuration command to enable authentication, authorization, and accounting (AAA) accounting and to create method lists defining specific accounting methods on a per-line or per-interface basis for IEEE 802.1x sessions. Use the **no** form of this command to disable IEEE 802.1x accounting.

**aaa accounting dot1x** {*name* | **default**} **start-stop** {**broadcast group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ... ] | **group** {*name* | **radius** | **tacacs+**} [**group** {*name* | **radius** | **tacacs+**} ... ]}

**no aaa accounting dot1x** {*name* | **default**}

**Syntax Description**

| | |
|---|---|
| *name* | Name of a server group. This is optional when you enter it after the **broadcast group** and **group** keywords. |
| **default** | Use the accounting methods that follow as the default list for accounting services. |
| **start-stop** | Send a start accounting notice at the beginning of a process and a stop accounting notice at the end of a process. The start accounting record is sent in the background. The requested-user process begins regardless of whether or not the start accounting notice was received by the accounting server. |
| **broadcast** | Enable accounting records to be sent to multiple AAA servers and send accounting records to the first server in each group. If the first server is unavailable, the switch uses the list of backup servers to identify the first server. |
| **group** | Specify the server group to be used for accounting services. These are valid server group names:<br>• *name*—Name of a server group.<br>• **radius**—List of all RADIUS hosts.<br>• **tacacs+**—List of all TACACS+ hosts.<br>The **group** keyword is optional when you enter it after the **broadcast group** and **group** keywords. You can enter more than optional **group** keyword. |

| | |
|---|---|
| **radius** | (Optional) Enable RADIUS authorization. |
| **tacacs+** | (Optional) Enable TACACS+ accounting. |

## Defaults

AAA accounting is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This command requires access to a RADIUS server.

**Note** We recommend that you enter the **dot1x reauthentication** interface configuration command before configuring IEEE 802.1x RADIUS accounting on an interface.

## Examples

This example shows how to configure IEEE 802.1x accounting:

```
Switch(config)# aaa accounting dot1x
Switch(config)# aaa accounting dot1x default start-stop group radius
Switch(config)#
```

**Note** The RADIUS authentication server must be properly configured to accept and log update or watchdog packets from the AAA client.

## Related Commands

| Command | Description |
|---|---|
| **aaa authentication dot1x** | Specifies one or more AAA methods for use on interfaces running IEEE 802.1x. |
| **aaa-new-model** | Enables the AAA access control model. For syntax information, see the **Cisco IOS Security Command Reference, Release 12.2> Authentication, Authorization, and Accounting > Authentication Commands**. |
| **dot1x reauthentication** | Enables or disables periodic re-authentication. |
| **dot1x timeout reauth period** | Sets the number of seconds between re-authentication attempts. |

# aaa authentication dot1x

Use the **aaa authentication dot1x** global configuration command to specify the authentication, authorization, and accounting (AAA) method to use on ports complying with IEEE 802.1x. Use the **no** form of this command to disable authentication.

**aaa authentication dot1x** {**default**} *method1*

**no aaa authentication dot1x** {**default**}

## Syntax Description

| | |
|---|---|
| **default** | Use the listed authentication method that follows this argument as the default method when a user logs in. |
| *method1* | Enter the **group radius** keywords to use the list of all RADIUS servers for authentication. |

**Note** Though other keywords are visible in the command-line help strings, only the **default** and **group radius** keywords are supported.

## Defaults

No authentication is performed.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The *method* argument identifies the method that the authentication algorithm tries in the given sequence to validate the password provided by the client. The only method that is truly IEEE 802.1x-compliant is the **group radius** method, in which the client data is validated against a RADIUS authentication server.

If you specify **group radius**, you must configure the RADIUS server by entering the **radius-server host** global configuration command.

Use the **show running-config** privileged EXEC command to display the configured lists of authentication methods.

## Examples

This example shows how to enable AAA and how to create an IEEE 802.1x-compliant authentication list. This authentication first tries to contact a RADIUS server. If this action returns an error, the user is not allowed access to the network.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **aaa new-model** | Enables the AAA access control model. For syntax information, see the **Cisco IOS Security Command Reference, Release 12.2 > Authentication, Authorization, and Accounting > Authentication Commands**. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# action

Use the **action** access-map configuration command to set the action for the VLAN access map entry. Use the **no** form of this command to set the action to the default value, which is to forward.

**action** {**drop** | **forward**}

**no action**

## Syntax Description

| | |
|---|---|
| **drop** | Drop the packet when the specified conditions are matched. |
| **forward** | Forward the packet when the specified conditions are matched. |

## Defaults

The default action is to forward packets.

## Command Modes

Access-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

If the action is **drop**, you should define the access map, including configuring any access control list (ACL) names in match clauses, before applying the map to a VLAN, or all packets could be dropped.

In access-map configuration mode, use the **match** access-map configuration command to define the match conditions for a VLAN map. Use the **action** command to set the action that occurs when a packet matches the conditions.

The drop and forward parameters are not used in the **no** form of the command.

## Examples

This example shows how to identify and apply a VLAN access map *vmap4* to VLANs 5 and 6 that causes the VLAN to forward an IP packet if the packet matches the conditions defined in access list *al2*:

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **access-list** {**deny** \| **permit**} | Configures a standard numbered ACL. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**. |
| **ip access-list** | Creates a named access list. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**. |
| **mac access-list extended** | Creates a named MAC address access list. |
| **match (access-map configuration)** | Defines the match conditions for a VLAN map. |
| **show vlan access-map** | Displays the VLAN access maps created on the switch. |
| **vlan access-map** | Creates a VLAN access map. |

# archive download-sw

Use the **archive download-sw** privileged EXEC command to download a new image from a TFTP server to the switch and to overwrite or keep the existing image.

**archive download-sw** {**/force-reload** | **/imageonly** | **/leave-old-sw** | **/no-set-boot** | **/no-version-check** | **/overwrite** | **/reload** | **/safe**} *source-url*

## Syntax Description

| | |
|---|---|
| **/force-reload** | Unconditionally force a system reload after successfully downloading the software image. |
| **/imageonly** | Download only the software image but not the HTML files associated with the embedded device manager. The HTML files for the existing version are deleted only if the existing version is being overwritten or removed. |
| **/leave-old-sw** | Keep the old software version after a successful download. |
| **/no-set-boot** | Do not alter the setting of the BOOT environment variable to point to the new software image after it is successfully downloaded. |
| **/no-version-check** | Download the software image without checking to prevent installing an incompatible image. |
| **/overwrite** | Overwrite the software image in flash memory with the downloaded one. |
| **/reload** | Reload the system after successfully downloading the image unless the configuration has been changed and not been saved. |
| **/safe** | Keep the current software image; do not delete it to make room for the new software image before the new image is downloaded. The current image is deleted after the download. |
| *source-url* | The source URL alias for a local or network file system. These options are supported:<br>• The syntax for the local flash file system: **flash:**<br>• The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***image-name***.tar**<br>• The syntax for an HTTP server: **http://**[[*username***:***password*]**@**]{*hostname* \| *host-ip*}[**/***directory*]**/***image-name***.tar**<br>• The syntax for a secure HTTP server: **https://**[[*username***:***password*]**@**]{*hostname* \| *host-ip*}[**/***directory*]**/***image-name***.tar**<br>• The syntax for the Remote Copy Protocol (RCP): **rcp:**[[**//***username***@***location*]**/***directory*]**/***image-name***.tar**<br>• The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar**<br>The *image-name***.tar** is the software image to download and install on the switch. |

**Defaults**

The current software image is not overwritten with the downloaded image.

Both the software image and HTML files are downloaded.

The new image is downloaded to the flash: file system.

The BOOT environment variable is changed to point to the new software image on the flash: file system.

Image names are case sensitive; the image file is provided in tar format.

Compatibility of the version on the image to be downloaded is checked.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

The **/imageonly** option removes the HTML files for the existing image if the existing image is being removed or replaced. Only the Cisco IOS image (without the HTML files) is downloaded.

Using the **/safe** or **/leave-old-sw** option can cause the new image download to fail if there is insufficient flash memory. If leaving the software in place prevents the new image from fitting in flash memory due to space constraints, an error results.

If you used the **/leave-old-sw** option and did not overwrite the old image when you downloaded the new one, you can remove the old image by using the **delete** privileged EXEC command. For more information, see the "delete" section on page 2-52.

**Note** Use the **/no-version-check** option with care. This option allows an image to be downloaded without first confirming that it is not incompatible with the switch.

Use the **/overwrite** option to overwrite the image on the flash device with the downloaded one.

If you specify the command *without* the **/overwrite** option, the download algorithm verifies that the new image is not the same as the one on the switch flash device. If the images are the same, the download does not occur. If the images are different, the old image is deleted, and the new one is downloaded.

After downloading a new image, enter the **reload** privileged EXEC command to begin using the new image, or specify the **/reload** or **/force-reload** option in the **archive download-sw** command.

**Examples**

This example shows how to download a new image from a TFTP server at 172.20.129.10 and overwrite the image on the switch:

```
Switch# archive download-sw /overwrite tftp://172.20.129.10/test-image.tar
```

This example shows how to download only the software image from a TFTP server at 172.20.129.10 to the switch:

```
Switch# archive download-sw /imageonly tftp://172.20.129.10/test-image.tar
```

This example shows how to keep the old software version after a successful download:

```
Switch# archive download-sw /leave-old-sw tftp://172.20.129.10/test-image.tar
```

**Related Commands**

| Command | Description |
|---|---|
| **archive tar** | Creates a tar file, lists the files in a tar file, or extracts the files from a tar file. |
| **archive upload-sw** | Uploads an existing image on the switch to a server. |
| **delete** | Deletes a file or directory on the flash memory device. |

# archive tar

Use the **archive tar** privileged EXEC command to create a tar file, list files in a tar file, or extract the files from a tar file.

**archive tar** {**/create** *destination-url* **flash:/***file-url*} | {**/table** *source-url*} | {**/xtract** *source-url* **flash:/***file-url* [*dir/file...*]}

## Syntax Description

| | |
|---|---|
| **/create** *destination-url* **flash:/***file-url* | Create a new tar file on the local or network file system.<br>For *destination-url, specify t*he destination URL alias for the local or network file system and the name of the tar file to create. These options are supported:<br>• The syntax for the local flash filesystem: **flash:**<br>• The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the Remote Copy Protocol (RCP) is: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**<br>The *tar-filename***.tar** is the tar file to be created.<br>For **flash:/***file-url, specify t*he location on the local flash file system from which the new tar file is created.<br>An optional list of files or directories within the source directory can be specified to write to the new tar file. If none are specified, all files and directories at this level are written to the newly created tar file. |
| **/table** *source-url* | Display the contents of an existing tar file to the screen.<br>For *source-url*, specify the source URL alias for the local or network file system. These options are supported:<br>• The syntax for the local flash file system: **flash:**<br>• The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**<br>The *tar-filename***.tar** is the tar file to display. |

| | |
|---|---|
| **/xtract** *source-url* **flash:/***file-url* [*dir/file...*] | Extract files from a tar file to the local file system.<br><br>For *source-url*, specify *t*he source URL alias for the local file system. These options are supported:<br><br>• The syntax for the local flash file system: **flash:**<br>• The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the RCP: **rcp:**[[**//***username***@***location*]**/***directory*]**/***tar-filename***.tar**<br>• The syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***tar-filename***.tar**<br><br>The *tar-filename***.tar** is the tar file from which to extract.<br><br>For **flash:/***file-url* [*dir/file...*], specify *t*he location on the local flash file system into which the tar file is extracted. Use the *dir/file...* option to specify an optional list of files or directories within the tar file to be extracted. If none are specified, all files and directories are extracted. |

## Defaults

None

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

Image names are case sensitive.

## Examples

This example shows how to create a tar file. The command writes the contents of the *new-configs* directory on the local flash device to a file named *saved.tar* on the TFTP server at 172.20.10.30:

```
Switch# archive tar /create tftp:172.20.10.30/saved.tar flash:/new-configs
```

This example shows how to display the contents of the file that is in flash memory. The contents of the tar file appear on the screen:

```
Switch# archive tar /table flash:me240x-metrobase-mz.122-25.EX.tar
info (219 bytes)
me240x-metrobase-mz.122-25.EX/(directory)
me240x-metrobase-mz.122-25.EX (610856 bytes)
me240x-metrobase-mz.122-25.EX/info (219 bytes)
info.ver (219 bytes)
```

This example shows how to display only the *html* directory and its contents:

```
Switch# archive tar /table flash:me240x-metrobase-mz.122-25.EX.tar me240x-metrobase-mz.12
-25/html
me240x-metrobase-mz.122-25.EX/html/ (directory)
me240x-metrobase-mz.122-25.EX/html/const.htm (556 bytes)
me240x-metrobase-mz.122-25.EX/html/xhome.htm (9373 bytes)
me240x-metrobase-mz.122-25.EX/html/menu.css (1654 bytes)
<output truncated>
```

This example shows how to extract the contents of a tar file on the TFTP server at 172.20.10.30. This command extracts just the *new-configs* directory into the root directory on the local flash file system. The remaining files in the *saved.tar* file are ignored.

```
Switch# archive tar /xtract tftp://172.20.10.30/saved.tar flash:/ new-configs
```

## Related Commands

| Command | Description |
|---|---|
| archive download-sw | Downloads a new image from a TFTP server to the switch. |
| archive upload-sw | Uploads an existing image on the switch to a server. |

# archive upload-sw

Use the **archive upload-sw** privileged EXEC command to upload an existing switch image to a server.

**archive upload-sw** [**/version** *version_string*] **destination-url**

## Syntax Description

| | |
|---|---|
| **/version** *version_string* | (Optional) Specify the specific version string of the image to be uploaded. |
| *destination-url* | The destination URL alias for a local or network file system. These options are supported:<br>• The syntax for the local flash file system: **flash:**<br>• The syntax for the FTP: **ftp:**[[**//***username*[**:***password*]**@***location*]**/***directory*]**/***image-name***.tar**<br>• The syntax for the Remote Copy Protocol (RCP): **rcp:**[[**//***username***@***location*]**/***directory*]**/***image-name***.tar**<br>• **T**he syntax for the TFTP: **tftp:**[[**//***location*]**/***directory*]**/***image-name***.tar**<br>The *image-name***.tar** is the name of software image to be stored on the server. |

## Defaults

Uploads the currently running image from the flash: file system.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the upload feature only if the HTML files associated with the embedded device manager have been installed with the existing image.

The files are uploaded in this sequence: the Cisco IOS image, the HTML files, and info. After these files are uploaded, the software creates the tar file.

Image names are case sensitive.

## Examples

This example shows how to upload the currently running image to a TFTP server at 172.20.140.2:

```
Switch# archive upload-sw tftp://172.20.140.2/test-image.tar
```

## Related Commands

| Command | Description |
|---|---|
| archive download-sw | Downloads a new image to the switch. |
| archive tar | Creates a tar file, lists the files in a tar file, or extracts the files from a tar file. |

# bandwidth

Use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) by setting the output bandwidth for a policy-map class. Use the **no** form of this command to remove the bandwidth setting for the class.

**bandwidth** {*rate* | **percent** *value* | **remaining percent** *value*}

**no bandwidth** [*rate* | **percent** *value* | **remaining percent** *value*]

## Syntax Description

| | |
|---|---|
| *rate* | Set the bandwidth rate for the class in kilobits per second (kbps). The range is from 64 to 1000000. |
| **percent** *value* | Set the bandwidth for the class as a percent of the total bandwidth. The range is from 1 to 100 percent. |
| **remaining percent** *value* | Set the bandwidth for the class as a percent of the remaining bandwidth. The range is from 1 to 100 percent. |

## Defaults

No bandwidth is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Support was added to configure the **bandwidth** command in the **class-default** of an output policy map. |

## Usage Guidelines

You use the **bandwidth** policy-map class command to control output traffic. The **bandwidth** command specifies the bandwidth for traffic in that class. CBWFQ derives the weight for packets belonging to the class from the bandwidth allocated to the class and uses the weight to ensure that the queue for that class is serviced fairly. Bandwidth settings are not supported in input policy maps.

When you configure bandwidth for a class of traffic as an absolute rate (kbps) or a percentage of bandwidth (**percent** *value)*, it represents the minimum bandwidth guarantee or committed information rate (CIR) for that traffic class. This means that the traffic class gets at least the bandwidth specified in the command, but is not limited to that bandwidth. Any excess bandwidth on the port is allocated to each class in the same ratio as the configured CIR rates.

When you enter the **bandwidth remaining percent** command, hard bandwidths are not guaranteed, and only relative bandwidths are assured. Class bandwidths are always proportional to the specified bandwidth percentages configured for the port.

When you configure bandwidth in an output policy, you must specify the same units in each bandwidth configuration; that is, all absolute values (rates) or percentages.

The total rate of the minimum bandwidth guarantees for each queue of the policy cannot exceed the total speed for the interface. If the **percent** keyword is used, the sum of the class bandwidth percentages cannot exceed 100 percent.

Using the **queue-limit** command to modify the default queue limit is especially important on higher-speed interfaces so that they meet the minimum bandwidth guarantees required by the interface.

You cannot use the **bandwidth** policy-map class configuration command to configure CBWFQ and the **shape average** command to configure class-based shaping for the same class in a policy map.

You cannot configure bandwidth in a class that includes priority queuing (configured with the **priority** policy-map class configuration command).

## Examples

This example shows how to set the precedence of output queues by setting bandwidth in kilobits per second. The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50000, 20000, and 10000 kbps. The class **class-default** at a minimum gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth 50000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth 20000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth 10000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to set the precedence of output queues by allocating percentages of the total available bandwidth to each traffic class.The classes *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent. The class **class-default** at a minimum gets 20 percent.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to set *outclass1* as a priority queue, with *outclass2*, and *outclass3* getting 50 and 20 percent, respectively, of the bandwidth remaining after the priority queue is serviced. The class **class-default** gets the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |

# boot boothlpr

Use the **boot boothlpr** global configuration command to load a special Cisco IOS image, which when loaded into memory, can load a second Cisco IOS image into memory and launch it. This variable is used only for internal development and testing. Use the **no** form of this command to return to the default setting.

**boot boothlpr** *filesystem***:/***file-url*

**no boot boothlpr**

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | The path (directory) and name of a bootable helper image. |

## Defaults

No helper image is loaded.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the BOOTHLPR environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands"

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot config-file

Use the **boot config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. Use the **no** form of this command to return to the default setting.

**boot config-file flash:***/file-url*

**no boot config-file**

## Syntax Description

| | |
|---|---|
| **flash:***/file-url* | The path (directory) and name of the configuration file. |

## Defaults

The default configuration file is flash:config.text.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

This command changes the setting of the CONFIG_FILE environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot enable-break

Use the **boot enable-break** global configuration command to enable interrupting the automatic boot process. Use the **no** form of this command to return to the default setting.

**boot enable-break**

**no boot enable-break**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Disabled. The automatic boot process cannot be interrupted by pressing the Break key on the console.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you enter this command, you can interrupt the automatic boot process by pressing the break key on the console after the flash file system is initialized. The break key is different for each operating system:

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

This command changes the setting of the ENABLE_BREAK environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot helper

Use the **boot helper** global configuration command to dynamically load files during boot loader initialization to extend or patch the functionality of the boot loader. Use the **no** form of this command to return to the default.

**boot helper** *filesystem*:*/file-url ...*

**no boot helper**

## Syntax Description

| | |
|---|---|
| *filesystem*: | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | The path (directory) and a list of loadable files to dynamically load during loader initialization. Separate each image name with a semicolon. |

## Defaults

No helper files are loaded.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot helper-config-file

Use the **boot helper-config-file** global configuration command to specify the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded. Use the **no** form of this command to return to the default setting.

**boot helper-config-file** *filesystem***:***/file-url*

**no boot helper-config file**

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | The path (directory) and helper configuration file to load. |

## Defaults

No helper configuration file is specified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This variable is used only for internal development and testing.

Filenames and directory names are case sensitive.

This command changes the setting of the HELPER_CONFIG_FILE environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot manual

Use the **boot manual** global configuration command to enable manually booting the switch during the next boot cycle. Use the **no** form of this command to return to the default setting.

**boot manual**

**no boot manual**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Manual booting is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The next time you reboot the system, the switch is in boot loader mode, which is shown by the *switch:* prompt. To boot the system, use the **boot** boot loader command, and specify the name of the bootable image.

This command changes the setting of the MANUAL_BOOT environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot private-config-file

Use the **boot private-config-file** global configuration command to specify the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration. Use the **no** form of this command to return to the default setting.

**boot private-config-file** *filename*

**no boot private-config-file**

## Syntax Description

| | |
|---|---|
| *filename* | The name of the private configuration file. |

## Defaults

The default configuration file is *private-config*.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames are case sensitive.

## Examples

This example shows how to specify the name of the private configuration file to be *pconfig*:

```
Switch(config)# boot private-config-file pconfig
```

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# boot system

Use the **boot system** global configuration command to specify the Cisco IOS image to load during the next boot cycle. Use the **no** form of this command to return to the default setting.

**boot system** f*ilesystem:/file-url* ...

**no boot system**

## Syntax Description

| | |
|---|---|
| *filesystem*: | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | The path (directory) and name of a bootable image. Separate image names with a semicolon. |

## Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

If you are using the **archive download-sw** privileged EXEC command to maintain system images, you never need to use the **boot system** command. The **boot system** command is automatically manipulated to load the downloaded image.

This command changes the setting of the BOOT environment variable. For more information, see Appendix A, "Cisco ME 2400 Ethernet Access Switch Boot Loader Commands."

## Related Commands

| Command | Description |
|---|---|
| **show boot** | Displays the settings of the boot environment variables. |

# channel-group

Use the **channel-group** interface configuration command to assign an Ethernet port to an EtherChannel group. Use the **no** form of this command to remove an Ethernet port from an EtherChannel group.

**channel-group** *channel-group-number* **mode** {**active** | {**auto** [**non-silent**] | **desirable** [**non-silent**] | **on**} | **passive**}

**no channel-group**

PAgP modes:
**channel-group** *channel-group-number* **mode** {**auto** [**non-silent**] | {**desirable** [**non-silent**]}

LACP modes:
**channel-group** *channel-group-number* **mode** {**active** | **passive**}

On mode:
**channel-group** *channel-group-number* **mode on**

**Note** Link Aggregation Control Protocol (LACP.) and Port Aggregation Protocol (PAgP) are available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs). The **active**, **auto**, **desirable**, and **passive** keywords are not visible on user network interfaces (UNIs).

## Syntax Description

| | |
|---|---|
| *channel-group-number* | Specify the channel group number. The range is 1 to 48. |
| **mode** | Specify the EtherChannel mode. |
| **active** | Unconditionally enable LACP<br>Active mode places a port into a negotiating state in which the port initiates negotiations with other ports by sending LACP packets. A channel is formed with another port group in either the active or passive mode. |
| **auto** | Enable the PAgP only if a PAgP device is detected.<br>Auto mode places a port into a passive negotiating state in which the port responds to PAgP packets it receives but does not start PAgP packet negotiation. A channel is formed only with another port group in desirable mode. When **auto** is enabled, silent operation is the default. |
| **desirable** | Unconditionally enable PAgP.<br>Desirable mode places a port into an active negotiating state in which the port starts negotiations with other ports by sending PAgP packets. A channel is formed with another port group in either the desirable or auto mode. When **desirable** is enabled, silent operation is the default. |
| **non-silent** | (Optional) Use in PAgP mode with the **auto** or **desirable** keyword when traffic is expected from the other device. |

| | |
|---|---|
| **on** | Enable **on** mode.<br>In **on** mode, a usable EtherChannel exists only when both connected port groups are in the **on** mode. |
| **passive** | Enable LACP only if a LACP device is detected.<br>Passive mode places a port into a negotiating state in which the port responds to LACP packets it receives but does not initiate LACP packet negotiation. A channel is formed only with another port group in active mode. |

## Defaults

No channel groups are assigned.

No mode is configured.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first by using the **interface port-channel** global configuration command before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port if the logical interface is not already created. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

If the port is a UNI or an ENI, you must use the **no shutdown** interface configuration command to enable it before using the **channel-group** command. UNIs and ENIs are disabled by default. NNIs are enabled by default.

After you configure an EtherChannel, configuration changes that you make on the port-channel interface apply to all the physical ports assigned to the port-channel interface. Configuration changes applied to the physical port affect only the port where you apply the configuration. To change the parameters of all ports in an EtherChannel, apply configuration commands to the port-channel interface, for example, spanning-tree commands or commands to configure a Layer 2 EtherChannel as a trunk.

If you do not specify **non-silent** with the **auto** or **desirable** mode, silent is assumed. The silent mode is used when the switch is connected to a device that is not PAgP-capable and seldom, if ever, sends packets. A example of a silent partner is a file server or a packet analyzer that is not generating traffic. In this case, running PAgP on a physical port prevents that port from ever becoming operational. However, it allows PAgP to operate, to attach the port to a channel group, and to use the port for transmission. Both ends of the link cannot be set to silent.

In the **on** mode, an EtherChannel exists only when a port group in the **on** mode is connected to another port group in the **on** mode.

**Caution** You should exercise care when setting the mode to **on** (manual configuration). All ports configured in the **on** mode are bundled in the same group and are forced to have similar characteristics. If the group is misconfigured, packet loss or spanning-tree loops might occur.

Do not configure an EtherChannel in both the PAgP and LACP modes. EtherChannel groups running PAgP and LACP can coexist on the same switch. Individual EtherChannel groups can run either PAgP or LACP, but they cannot interoperate.

**Note** PAgP and LACP are available only on NNIs and ENIs.

If you set the protocol by using the **channel-protocol** interface configuration command, the setting is not overridden by the **channel-group** interface configuration command.

Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.

Do not configure a secure port as part of an EtherChannel or an EtherChannel port as a secure port.

For a complete list of configuration guidelines, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

## Examples

This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the PAgP mode **desirable**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode desirable
Switch(config-if-range)# end
```

This example shows how to configure an EtherChannel. It assigns two static-access ports in VLAN 10 to channel 5 with the LACP mode **active**:

```
Switch# configure terminal
Switch(config)# interface range gigabitethernet0/1 -2
Switch(config-if-range)# switchport mode access
Switch(config-if-range)# switchport access vlan 10
Switch(config-if-range)# channel-group 5 mode active
Switch(config-if-range)# end
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **channel-protocol** | Restricts the protocol used on a port to manage channeling. |
| **interface port-channel** | Accesses or creates the port channel. |
| **show etherchannel** | Displays EtherChannel information for a channel. |
| **show lacp** | Displays LACP channel-group information. |
| **show pagp** | Displays PAgP channel-group information. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# channel-protocol

Use the **channel-protocol** interface configuration command to restrict the protocol used on a port to manage channeling. Use the **no** form of this command to return to the default setting.

**channel-protocol** {**lacp** | **pagp**}

**no channel-protocol**

## Syntax Description

| | |
|---|---|
| **lacp** | Configure an EtherChannel with the Link Aggregation Control Protocol (LACP). |
| **pagp** | Configure an EtherChannel with the Port Aggregation Protocol (PAgP). |

## Defaults

No protocol is assigned to the EtherChannel.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **channel-protocol** command only to restrict a channel to LACP or PAgP. If you set the protocol by using the **channel-protocol** command, the setting is not overridden by the **channel-group** interface configuration command.

**Note** PAgP and LACP are available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

If the port is a user network interface (UNI) or an ENI, you must use the **no shutdown** interface configuration command to enable it before using the **channel-protocol** command. UNIs and ENIs are disabled by default. NNIs are enabled by default.

You must use the **channel-group** interface configuration command to configure the EtherChannel parameters. The **channel-group** command also can set the mode for the EtherChannel.

You cannot enable both the PAgP and LACP modes on an EtherChannel group.

PAgP and LACP are not compatible; both ends of a channel must use the same protocol.

## Examples

This example shows how to specify LACP as the protocol that manages the EtherChannel:

```
Switch(config-if)# channel-protocol lacp
```

You can verify your settings by entering the **show etherchannel** [*channel-group-number*] **protocol** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **channel-group** | Assigns an Ethernet port to an EtherChannel group. |
| **show etherchannel protocol** | Displays protocol information the EtherChannel. |

# class

Use the **class** policy-map configuration command to specify the name of the class whose policy you want to create or to change or to specify the system default class before you configure a policy and to enter policy-map class configuration mode. Use the **no** form of this command to remove the class from a policy map.

**class** {*class-map-name*| **class-default**}

**no class** {*class-map-name*| **class-default**}

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of a class map created by using the **class-map** global configuration command. |
| **class-default** | The system default class. This class matches all unclassified traffic. You cannot create or delete the default class. |

## Defaults

No policy map classes are defined.

## Command Modes

Policy-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Before using the **class** *class-map-name* command in policy-map configuration mode, you must create the class by using the **class-map** *class-map-name* global configuration command. The class **class-default** is the class to which traffic is directed if that traffic does not match any of the match criteria in the configured class maps.

Use the **policy-map** global configuration command to identify the policy map and to enter policy-map configuration mode. After specifying a policy map, you can configure a policy for new classes or modify a policy for any existing classes in that policy map.

An input policy map can have a maximum of 32 classes, one of which is **class-default**.

You attach the policy map to a port by using the **service-policy** interface configuration command.

After entering the **class** command, you enter policy-map class configuration mode, and these configuration commands are available:

- **bandwidth**: specifies the bandwidth allocated for a class belonging to a policy map. For more information, see the **bandwidth** command.
- **exit**: exits policy-map class configuration mode and returns to policy-map configuration mode.
- **no**: returns a command to its default setting.

- **police**: defines an individual policer or aggregate policer for the classified traffic. The policer specifies the bandwidth limitations and the action to take when the limits are exceeded. For more information, see the **police** and **police aggregate (policy-map class configuration)** policy-map class commands.
- **priority**: sets the strict scheduling priority for this class or, when used with the **police** keyword, sets priority with police. For more information, see the **priority** policy-map class command.
- **queue-limit**: sets the queue maximum threshold for Weighted Tail Drop (WTD). For more information, see the **queue-limit** command.
- **service-policy**: configures a QoS service policy to attach to a parent policy map for an input or output policy. For more information, see the **service-policy (policy-map class configuration)** command.
- **set**: specifies a value to be assigned to the classified traffic. For more information, see the **set** commands.
- **shape average**: specifies the average traffic shaping rate. For more information, see the **shape average** command.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to create a policy map called *policy1,* define a class *class1*, and enter policy-map class configuration mode to set a criterion for the class.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |
| **show policy-map interface** [*interface-id*] | Displays policy maps configured on the specified interface or on all interfaces. |

# class-map

Use the **class-map** global configuration command to create a class map to be used for matching packets to a specified criteria and to enter class-map configuration mode. Use the **no** form of this command to delete an existing class map.

**class-map** [**match-all** | **match-any**] *class-map-name*

**no class-map** [**match-all** | **match-any**] *class-map-name*

## Syntax Description

| | |
|---|---|
| **match-all** | (Optional) Perform a logical-AND of all matching statements under this class map. Packets must meet all of the match criteria. |
| **match-any** | (Optional) Perform a logical-OR of the matching statements under this class map. Packets must meet one or more of the match criteria. |
| *class-map-name* | Name of the class map. |

## Defaults

No class maps are defined.

If neither the **match-all** or the **match-any** keyword is specified, the default is **match-all**.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to specify the name of the class for which you want to create or to modify class-map match criteria and to enter class-map configuration mode.

The switch supports a maximum of 256 unique class maps.

You use the **class-map** command and class-map configuration mode to define packet classification as part of a globally named service policy applied on a per-port basis. When you configure a class map, you can use one or more **match** commands to specify match criteria. Packets arriving at either the input or output interface (determined by how you configure the **service-policy** interface configuration command) are checked against the class-map match criteria to determine if the packet belongs to that class.

A **match-all** class map means that the packet must match all entries and can have no other match statements.

After you are in class-map configuration mode, these configuration commands are available:

- **description**: describes the class map (up to 200 characters). The **show class-map** privileged EXEC command displays the description and the name of the class map.
- **exit**: exits QoS class-map configuration mode.
- **match**: configures classification criteria. For more information, see the **match** class-map configuration commands.
- **no**: removes a match statement from a class map.

## Examples

This example shows how to configure the class map called *class1*. By default, the class map is **match-all** and therefore can contain no other match criteria.

```
Switch(config)# class-map class1
Switch(config-cmap)# exit
```

This example shows how to configure a match-any class map with one match criterion, which is an access list called *103*. This class map (matching an ACL) is supported only in an input policy map.

```
Switch(config)# class-map class2
Switch(config-cmap)# match access-group 103
Switch(config-cmap)# exit
```

This example shows how to delete the class map ***class1***:

```
Switch(config)# no class-map class1
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **match access-group** | Configures the match criteria for a class map on the basis of the specified access control list (ACL) |
| **match cos** | Configures the match criteria for a class map on the basis of the Layer 2 class of service (CoS) marking, |
| **match ip dscp** | Configures the match criteria for a class map on the basis of a specific IPv4 Differentiated Service Code Point (DSCP) value. |
| **match ip precedence** | Configures the match criteria for a class map on the basis of IPv4 precedence values. |
| **match qos-group** | Configures the match criteria for a class map on the basis of a specific quality of service (QoS) group value. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show class-map** | Displays QoS class maps. |

# clear ip dhcp snooping

Use the **clear ip dhcp snooping** privileged EXEC command to clear the DHCP binding database agent statistics or the DHCP snooping statistics counters.

**clear ip dhcp snooping** {**binding** {***** | *ip-address* | **interface** *interface-id* | **vlan** *vlan-id*} | **database statistics** | **statistics**}

## Syntax Description

| | |
|---|---|
| **binding** | Clear the DHCP snooping binding database. |
| ***** | Clear all automatic bindings. |
| *ip-address* | Clear the binding entry IP address. |
| **interface** *interface-id* | Clear the binding input interface. |
| **vlan** *vlan-id* | Clear the binding entry VLAN. |
| **database statistics** | Clear the DHCP snooping binding database agent statistics. |
| **database statistics** | Clear the DHCP snooping binding database agent statistics. |
| **statistics** | Clear the DHCP snooping statistics counter. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(37)SE | The **statistics** keyword was introduced. |
| 12.2(44)SE | The *****, *ip-address,* **interface** *interface-id,* and **vlan** *vlan-id* keywords were introduced. |

## Usage Guidelines

When you enter the **clear ip dhcp snooping database statistics** command, the switch does not update the entries in the binding database and in the binding file before clearing the statistics.

## Examples

This example shows how to clear the DHCP snooping binding database agent statistics:

```
Switch# clear ip dhcp snooping database statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping database** privileged EXEC command.

This example shows how to clear the DHCP snooping statistics counters:

```
Switch# clear ip dhcp snooping statistics
```

You can verify that the statistics were cleared by entering the **show ip dhcp snooping statistics** user EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables DHCP snooping on a VLAN. |
| **ip dhcp snooping database** | Configures the DHCP snooping binding database agent or the binding file. |
| **show ip dhcp snooping binding** | Displays the status of DHCP snooping database agent. |
| **show ip dhcp snooping database** | Displays the DHCP snooping binding database agent statistics. |
| **show ip dhcp snooping statistics** | Displays the DHCP snooping statistics. |

# clear lacp

Use the **clear lacp** privileged EXEC command to clear Link Aggregation Control Protocol (LACP) channel-group counters.

**clear lacp** {*channel-group-number* **counters** | **counters**}

**Note** LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *channel-group-number* | (Optional) Channel group number. The range is 1 to 48. |
| **counters** | Clear traffic counters. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can clear all counters by using the **clear lacp counters** command, or you can clear only the counters for the specified channel group by using the **clear lacp** *channel-group-number* **counters** command.

## Examples

This example shows how to clear all channel-group information:

```
Switch# clear lacp counters
```

This example shows how to clear LACP traffic counters for group 4:

```
Switch# clear lacp 4 counters
```

You can verify that the information was deleted by entering the **show lacp counters** or the **show lacp 4 counters** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show lacp** | Displays LACP channel-group information. |

# clear mac address-table

Use the **clear mac address-table** privileged EXEC command to delete from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. This command also clears the MAC address notification global counters.

**clear mac address-table** {**dynamic** [**address** *mac-addr* | **interface** *interface-id* | **vlan** *vlan-id*] | **notification**}

## Syntax Description

| | |
|---|---|
| **dynamic** | Delete all dynamic MAC addresses. |
| **dynamic address** *mac-addr* | (Optional) Delete the specified dynamic MAC address. |
| **dynamic interface** *interface-id* | (Optional) Delete all dynamic MAC addresses on the specified physical port or port channel. |
| **dynamic vlan** *vlan-id* | (Optional) Delete all dynamic MAC addresses for the specified VLAN. The range is 1 to 4096. |
| **notification** | Clear the notifications in the history table and reset the counters. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to remove a specific MAC address from the dynamic address table:

```
Switch# clear mac address-table dynamic address 0008.0070.0007
```

You can verify that the information was deleted by entering the **show mac address-table** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **mac address-table notification** | Enables the MAC address notification feature. |
| **show mac address-table** | Displays the MAC address table static and dynamic entries. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **snmp trap mac-notification** | Enables the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific interface. |

# clear pagp

Use the **clear pagp** privileged EXEC command to clear Port Aggregation Protocol (PAgP) channel-group information.

**clear pagp** {*channel-group-number* **counters** | **counters**}

**Note** PAgP is available only on network node interfaces (NNIs) enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *channel-group-number* | (Optional) Channel group number. The range is 1 to 48. |
| **counters** | Clear traffic counters. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can clear all counters by using the **clear pagp counters** command, or you can clear only the counters for the specified channel group by using the **clear pagp** *channel-group-number* **counters** command.

## Examples

This example shows how to clear all channel-group information:

```
Switch# clear pagp counters
```

This example shows how to clear PAgP traffic counters for group 10:

```
Switch# clear pagp 10 counters
```

You can verify that information was deleted by entering the **show pagp** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show pagp** | Displays PAgP channel-group information. |

# clear policer cpu uni-eni counters

Use the **clear policer cpu uni-eni counters** privileged EXEC command to clear control-plane policer statistics. The control-plane policer drops or rate-limits control packets from user network interfaces (UNIs) and enhanced network interfaces (ENIs) to protect the CPU from overload.

**clear policer cpu uni-eni counters** {**classification** | **drop**}

## Syntax Description

| | |
|---|---|
| **classification** | Clear control-plane policer classification counters that maintain statistics by feature. |
| **drop** | Clear all frame drop statistics maintained by the control-plane policer. |

## Command Default

No default is defined.

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(44)SE | The **uni** keyword was changed to **uni-eni**. |

## Usage Guidelines

You can use this command to clear statistics maintained per feature or statistics about dropped frames.

You can enter the **show platform policer cpu classification** or **show policer cpu uni drop** command to view feature statistics or dropped frames before and after you use the **clear** command.

## Related Commands

| Command | Description |
|---|---|
| **show platform policer cpu classification** | Displays CPU policer statistics per feature. |
| **show policer cpu uni-eni** | Displays CPU policer information for the switch. |

# clear port-security

Use the **clear port-security** privileged EXEC command to delete from the MAC address table all secure addresses or all secure addresses of a specific type (configured, dynamic, or sticky) on the switch or on an interface.

**clear port-security** {**all** | **configured** | **dynamic** | **sticky**} [[**address** *mac-addr* | **interface** *interface-id*] [**vlan** {*vlan-id* | {**access** | **voice**}}]]

## Syntax Description

| | |
|---|---|
| **all** | Delete all secure MAC addresses. |
| **configured** | Delete configured secure MAC addresses. |
| **dynamic** | Delete secure MAC addresses auto-learned by hardware. |
| **sticky** | Delete secure MAC addresses, either auto-learned or configured. |
| **address** *mac-addr* | (Optional) Delete the specified dynamic secure MAC address. |
| **interface** *interface-id* | (Optional) Delete all the dynamic secure MAC addresses on the specified physical port or VLAN. |
| **vlan** | (Optional) Delete the specified secure MAC address from the specified VLAN. Enter one of these options after you enter the **vlan** keyword:<br>• *vlan-id*—On a trunk port, specify the VLAN ID of the VLAN on which this address should be cleared.<br>• **access**—On an access port, clear the specified secure MAC address on the access VLAN. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to clear all secure addresses from the MAC address table:

```
Switch# clear port-security all
```

This example shows how to remove a specific configured secure address from the MAC address table:

```
Switch# clear port-security configured address 0008.0070.0007
```

This example shows how to remove all the dynamic secure addresses learned on a specific interface:

```
Switch# clear port-security dynamic interface gigabitethernet0/1
```

This example shows how to remove all the dynamic secure addresses from the address table:

```
Switch# clear port-security dynamic
```

You can verify that the information was deleted by entering the **show port-security** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **switchport port-security** | Enables port security on an interface. |
| **switchport port-security mac-address** *mac-address* | Configures secure MAC addresses. |
| **switchport port-security maximum** *value* | Configures a maximum number of secure MAC addresses on a secure interface. |
| **show port-security** | Displays the port security settings defined for an interface or for the switch. |

# clear spanning-tree counters

Use the **clear spanning-tree counters** privileged EXEC command to clear the spanning-tree counters.

**clear spanning-tree counters** [**interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Clear all spanning-tree counters on the specified interface. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs) on which spanning tree has been enabled, VLANs, and spanning-tree port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.<br>**Note** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs or on ENIs on which STP is not enabled. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the *interface-id* is not specified, spanning-tree counters are cleared for all STP ports.

## Examples

This example shows how to clear spanning-tree counters for all STP ports:

```
Switch# clear spanning-tree counters
```

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree** | Displays spanning-tree state information. |

# clear spanning-tree detected-protocols

Use the **clear spanning-tree detected-protocols** privileged EXEC command to restart the protocol migration process (force the renegotiation with neighboring switches) on all spanning-tree interfaces or on the specified interface.

**clear spanning-tree detected-protocols** [**interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Restart the protocol migration process on the specified interface. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs) on which spanning tree is enabled, VLANs, and port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.<br>**Note** Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). Though visible in the command-line help, the command has no effect on UNIs or on ENIs on which STP is not enabled. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A switch running the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol or the Multiple Spanning Tree Protocol (MSTP) supports a built-in protocol migration mechanism that enables it to interoperate with legacy IEEE 802.1D switches. If a rapid-PVST+ switch or an MSTP switch receives a legacy IEEE 802.1D configuration bridge protocol data unit (BPDU) with the protocol version set to 0, it sends only IEEE 802.1D BPDUs on that port. A multiple spanning-tree (MST) switch can also detect that a port is at the boundary of a region when it receives a legacy BPDU, an MST BPDU (Version 3) associated with a different region, or a rapid spanning-tree (RST) BPDU (Version 2).

However, the switch does not automatically revert to the rapid-PVST+ or the MSTP mode if it no longer receives IEEE 802.1D BPDUs. It cannot learn whether the legacy switch has been removed from the link unless the legacy switch is the designated switch. Use the **clear spanning-tree detected-protocols** command in this situation.

## Examples

This example shows how to restart the protocol migration process on a port:

```
Switch# clear spanning-tree detected-protocols interface gigabitethernet0/1
```

## Related Commands

| Command | Description |
|---|---|
| show spanning-tree | Displays spanning-tree state information. |
| spanning-tree link-type | Overrides the default link-type setting and enables rapid spanning-tree transitions to the forwarding state. |

# clear vmps statistics

Use the **clear vmps statistics** privileged EXEC command to clear the statistics maintained by the VLAN Query Protocol (VQP) client.

**clear vmps statistics**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to clear VLAN Membership Policy Server (VMPS) statistics:

```
Switch# clear vmps statistics
```

You can verify that information was deleted by entering the **show vmps statistics** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show vmps | Displays the VQP version, reconfirmation interval, retry count, VMPS IP addresses, and the current and primary servers. |

# conform-action

Use the **conform-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets that conform to the committed information rate (CIR). Use the **no** form of this command to cancel the action or return to the default action.

**conform-action** {**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

**no conform-action** {**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

## Syntax Description

| | |
|---|---|
| **set-cos-transmit** *new-cos-value* | Set a new class of service (CoS) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new CoS value is 0 to 7. |
| **set-dscp-transmit** *new-dscp-value* | Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new DCSP value is 0 to 63. |
| **set-prec-transmit** *new-precedence-value* | Set a new IP precedence value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new IP precedence value is 0 to 7. |
| **set-qos-transmit** *qos-group-value* | Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new QoS value is 0 to 99. |
| **cos** | (Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **dscp** | (Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **precedence** | (Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **table** *table-map name* | (Optional) Used in conjunction with the preceding *from-type* keyword. Specify the table map to be used for the enhanced packet marking. The *to-type* of the action is marked based on the *from-type* parameter of the action using this table map. |
| **transmit** | (Optional) Send the packet unmodified. |

## Defaults

The default conform action is to send the packet.

## Command Modes

Policy-map class police configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Increased support for configuring conform-action marking. See "Usage Guidelines." |

## Usage Guidelines

Beginning with Cisco IOS release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking, which provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class and configure conromf0action marking and exceed-action marking simultaneously.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

Use this command to set one or more conform actions for a traffic class.

## Examples

This example shows how configure multiple conform actions in a policy map that sets a committed information rate of 23000 bits per second (bps) and a conform burst rate of 10000 bps. The policy map includes multiple conform actions (for DSCP and for Layer 2 CoS) and an exceed action.

```
Switch(config)# policy-map map1
Switch(config-pmap)# class cos-set-1
Switch(config-pmap-c)# police cir 23000 bc 10000
Switch(config-pmap-c-police)# conform-action set-dscp-transmit 48
Switch(config-pmap-c-police)# conform-action set-cos-transmit 5
Switch(config-pmap-c-police)# exceed-action drop
Switch(config-pmap-c-police)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **exceed-action** | Defines the action to take on traffic that exceeds the CIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **police** | Defines a policer for classified traffic. |
| **show policy-map** | Displays QoS policy maps. |

# define interface-range

Use the **define interface-range** global configuration command to create an interface-range macro. Use the **no** form of this command to delete the defined macro.

**define interface-range** *macro-name interface-range*

**no define interface-range** *macro-name interface-range*

## Syntax Description

| | |
|---|---|
| *macro-name* | Name of the interface-range macro; up to 32 characters. |
| *interface-range* | Interface range; for valid values for interface ranges, see "Usage Guidelines." |

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The macro name is a 32-character maximum character string.

A macro can contain up to five ranges.

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs, but you can combine multiple interface types in a macro.

When entering the *interface-range*, use this format:

- *type* {*first-interface*} - {*last-interface*}
- You must add a space between the first interface number and the hyphen when entering an *interface-range*. For example, **gigabitethernet 0/1 - 2** is a valid range; **gigabitethernet 0/1-2** is not a valid range

Valid values for *type* and *interface*:

- **vlan** *vlan-id*, where *vlan-id* is from 1 to 4094

  VLAN interfaces must have been configured with the **interface vlan** command (the **show running-config** privileged EXEC command displays the configured VLAN interfaces). VLAN interfaces not displayed by the **show running-config** command cannot be used in *interface-ranges.*
- **port-channel** *port-channel-number*, where *port-channel-number* is from 1 to 48
- **fastethernet** *module*/{*first port*} - {*last port*}
- **gigabitethernet** *module*/{*first port*} - {*last port*}

For physical interfaces:

- module is always 0.
- the range is *type* **0**/*number* - *number* (for example, **gigabitethernet 0/1 - 2**).

When you define a range, you must enter a space before the hyphen (-), for example:

**gigabitethernet0/1 - 2**

You can also enter multiple ranges. When you define multiple ranges, you must enter a space after the first entry before the comma (,). The space after the comma is optional, for example:

**fastethernet0/3, gigabitethernet0/1 - 2**

**fastethernet0/3 -4, gigabitethernet0/1 - 2**

## Examples

This example shows how to create a multiple-interface macro:

```
Switch(config)# define interface-range macro1 fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

## Related Commands

| Command | Description |
|---|---|
| **interface range** | Executes a command on multiple ports at the same time. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# delete

Use the **delete** privileged EXEC command to delete a file or directory on the flash memory device.

**delete** [**/force**] [**/recursive**] *filesystem***:***/file-url*

## Syntax Description

| | |
|---|---|
| **/force** | (Optional) Suppress the prompt that confirms the deletion. |
| **/recursive** | (Optional) Delete the named directory and all subdirectories and the files contained in it. |
| *filesystem***:** | Alias for a flash file system.<br>The syntax for the local flash file system:<br>**flash:** |
| */file-url* | The path (directory) and filename to delete. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you use the **/force** keyword, you are prompted once at the beginning of the deletion process to confirm the deletion.

If you use the **/recursive** keyword without the **/force** keyword, you are prompted to confirm the deletion of every file.

The prompting behavior depends on the setting of the **file prompt** global configuration command. By default, the switch prompts for confirmation on destructive file operations. For more information about this command, see the *Cisco IOS Command Reference for Release 12.1*.

## Examples

This example shows how to remove the directory that contains the old software image after a successful download of a new image:

```
Switch# delete /force /recursive flash:/old-image
```

You can verify that the directory was removed by entering the **dir** *filesystem***:** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **archive download-sw** | Downloads a new image to the switch and overwrites or keeps the existing image. |

# deny (MAC access-list configuration)

Use the **deny** MAC access-list configuration command to prevent non-IP traffic from being forwarded if the conditions are matched. Use the **no** form of this command to remove a deny condition from the named MAC access list.

{**deny** | **permit**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* |**mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

**no** {**deny** | **permit**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **aarp** | **amber** | **cos** *cos* | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

## Syntax Description

| | |
|---|---|
| **any** | Keyword to specify to deny any source or destination MAC address. |
| **host** *src MAC-addr* \| *src-MAC-addr mask* | Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied. |
| **host** *dst-MAC-addr* \| *dst-MAC-addr mask* | Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied. |
| *type mask* | (Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.<br>The *type* is 0 to 65535, specified in hexadecimal.<br>The *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match. |
| **aarp** | (Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. |
| **amber** | (Optional) Select EtherType DEC-Amber. |
| **cos** *cos* | (Optional) Select a class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message reminds the user if the **cos** option is configured. |
| **dec-spanning** | (Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree. |
| **decnet-iv** | (Optional) Select EtherType DECnet Phase IV protocol. |
| **diagnostic** | (Optional) Select EtherType DEC-Diagnostic. |
| **dsm** | (Optional) Select EtherType DEC-DSM. |
| **etype-6000** | (Optional) Select EtherType 0x6000. |
| **etype-8042** | (Optional) Select EtherType 0x8042**.** |
| **lat** | (Optional) Select EtherType DEC-LAT. |
| **lavc-sca** | (Optional) Select EtherType DEC-LAVC-SCA. |

| | |
|---|---|
| **lsap** *lsap-number mask* | (Optional) Use the LSAP number (0 to 65535) of a packet with IEEE 802.2 encapsulation to identify the protocol of the packet.<br><br>*mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match. |
| **mop-console** | (Optional) Select EtherType DEC-MOP Remote Console. |
| **mop-dump** | (Optional) Select EtherType DEC-MOP Dump. |
| **msdos** | (Optional) Select EtherType DEC-MSDOS. |
| **mumps** | (Optional) Select EtherType DEC-MUMPS. |
| **netbios** | (Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS). |
| **vines-echo** | (Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems. |
| **vines-ip** | (Optional) Select EtherType VINES IP. |
| **xns-idp** | (Optional) Select EtherType Xerox Network Systems (XNS) protocol suite (0 to 65535), an arbitrary Ethertype in decimal, hexadecimal, or octal. |

**Note** Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-1.

***Table 2-1 IPX Filtering Criteria***

| **IPX Encapsulation Type** | | |
|---|---|---|
| **Cisco IOS Name** | **Novel Name** | **Filter Criterion** |
| arpa | Ethernet II | Ethertype 0x8137 |
| snap | Ethernet-snap | Ethertype 0x8137 |
| sap | Ethernet 802.2 | LSAP 0xE0E0 |
| novell-ether | Ethernet 802.3 | LSAP 0xFFFF |

## Defaults

This command has no defaults. However; the default action for a MAC-named ACL is to deny.

## Command Modes

MAC-access list configuration

## Command History

| **Release** | **Modification** |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You enter MAC-access list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **host** keyword, you must enter an address mask.

When an access control entry (ACE) is added to an access control list, an implied **deny-any-any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

**Note** For more information about named MAC extended access lists, see the software configuration guide for this release.

## Examples

This example shows how to define the named MAC extended access list to deny NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is denied.

```
Switch(config-ext-macl)# deny any host 00c0.00a0.03fa netbios.
```

This example shows how to remove the deny condition from the named MAC extended access list:

```
Switch(config-ext-macl)# no deny any 00c0.00a0.03fa 0000.0000.0000 netbios.
```

This example denies all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# deny any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **mac access-list extended** | Creates an access list based on MAC addresses for non-IP traffic. |
| **permit (MAC access-list configuration)** | Permits non-IP traffic to be forwarded if conditions are matched. |
| **show access-lists** | Displays access control lists configured on a switch. |

# dot1x default

Use the **dot1x default** interface configuration command to reset the configurable IEEE 802.1x parameters to their default values.

**dot1x default**

## Syntax Description

This command has no arguments or keywords.

## Defaults

These are the default values:

- The per-port IEEE 802.1x protocol enable state is disabled (force-authorized).
- The number of seconds between re-authentication attempts is 3600 seconds.
- The periodic re-authentication is disabled.
- The quiet period is 60 seconds.
- The retransmission time is 30 seconds.
- The maximum retransmission number is 2 times.
- The host mode is single host.
- The client timeout period is 30 seconds.
- The authentication server timeout period is 30 seconds.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to reset the configurable IEEE 802.1x parameters on a port:

```
Switch(config-if)# dot1x default
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x host-mode

Use the **dot1x host-mode** interface configuration command to allow a single host (client) or multiple hosts on an IEEE 802.1x-authorized port that has the **dot1x port-control** interface configuration command set to **auto**. Use the **no** form of this command to return to the default setting.

**dot1x host-mode** {**multi-host** | **single-host**}

**no dot1x host-mode** [**multi-host** | **single-host**]

## Syntax Description

| | |
|---|---|
| **multi-host** | Enable multiple-hosts mode on the switch. |
| **single-host** | Enable single-host mode on the switch. |

## Defaults

The default is single-host mode.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to limit an IEEE 802.1x-enabled port to a single client or to attach multiple clients to an IEEE 802.1x-enabled port. In multiple-hosts mode, only one of the attached hosts must be successfully authorized for all hosts to be granted network access. If the port becomes unauthorized (re-authentication fails or an Extensible Authentication Protocol over LAN [EAPOL]-logoff message is received), all attached clients are denied access to the network.

Before entering this command, make sure that the **dot1x port-control** interface configuration command is set to **auto** for the specified port.

## Examples

This example shows how to enable IEEE 802.1x globally, to enable IEEE 802.1x on a port, and to enable multiple-hosts mode:

```
Switch(config)# dot1x system-auth-control
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
Switch(config-if)# dot1x host-mode multi-host
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x initialize

Use the **dot1x initialize** privileged EXEC command to manually return the specified IEEE 802.1x-enabled port to an unauthorized state before initiating a new authentication session on the port.

**dot1x initialize interface** *interface-id*

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | Port to be initialized. |

## Defaults

There is no default setting.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to initialize the IEEE 802.1x state machines and to set up a fresh environment for authentication. After you enter this command, the port status becomes unauthorized.

There is no **no** form of this command.

## Examples

This example shows how to manually initialize a port:

```
Switch# dot1x initialize interface gigabitethernet0/2
```

You can verify the unauthorized port status by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x max-reauth-req

Use the **dot1x max-reauth-req** interface configuration command to set the maximum number of times that the switch restarts the authentication process before a port transitions to the unauthorized state. Use the **no** form of this command to return to the default setting.

**dot1x max-reauth-req** *count*

**no dot1x max-reauth-req**

## Syntax Description

| | |
|---|---|
| *count* | Number of times that the switch restarts the authentication process before the port transitions to the unauthorized state. The range is 1 to 10. |

## Defaults

The default is 2 times.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

## Examples

This example shows how to set 4 as the number of times that the switch restarts the authentication process before the port transitions to the unauthorized state:

```
Switch(config-if)# dot1x max-reauth-req 4
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x max-req** | Sets the maximum number of times that the switch forwards an EAP frame (assuming that no response is received) to the authentication server before restarting the authentication process. |
| **dot1x timeout tx-period** | Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. |
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x max-req

Use the **dot1x max-req** interface configuration command to set the maximum number of times that the switch sends an Extensible Authentication Protocol (EAP) frame from the authentication server (assuming that no response is received) to the client before restarting the authentication process. Use the **no** form of this command to return to the default setting.

**dot1x max-req** *count*

**no dot1x max-req**

## Syntax Description

| | |
|---|---|
| *count* | Number of times that the switch resends an EAP frame from the authentication server before restarting the authentication process. The range is 1 to 10. |

## Defaults

The default is 2 times.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

## Examples

This example shows how to set 5 as the number of times that the switch sends an EAP frame from the authentication server before restarting the authentication process:

```
Switch(config-if)# dot1x max-req 5
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x timeout tx-period** | Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before resending the request. |
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x port-control

Use the **dot1x port-control** interface configuration command to enable manual control of the authorization state of the port. Use the **no** form of this command to return to the default setting.

**dot1x port-control** {**auto** | **force-authorized** | **force-unauthorized**}

**no dot1x port-control**

## Syntax Description

| | |
|---|---|
| **auto** | Enable IEEE 802.1x authentication on the port and cause the port to change to the authorized or unauthorized state based on the IEEE 802.1x authentication exchange between the switch and the client. |
| **force-authorized** | Disable IEEE 802.1x authentication on the port and cause the port to change to the authorized state without an authentication exchange. The port sends and receives normal traffic without IEEE 802.1x-based authentication of the client. |
| **force-unauthorized** | Deny all access through this port by forcing the port to change to the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the port. |

## Defaults

The default is force-authorized.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You must globally enable IEEE 802.1x on the switch by using the **dot1x system-auth-control** global configuration command before enabling IEEE 802.1x on a specific port.

You can use the **auto** keyword only if the port is not configured as one of these:

- Trunk port—If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, an error message appears, and the port mode is not changed.
- Dynamic-access ports—If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

- EtherChannel port—Do not configure a port that is an active or a not-yet-active member of an EtherChannel as an IEEE 802.1x port. If you try to enable IEEE 802.1x on an EtherChannel port, an error message appears, and IEEE 802.1x is not enabled.
- Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) destination ports—You can enable IEEE 802.1x on a port that is a SPAN or RSPAN destination port. However, IEEE 802.1x is disabled until the port is removed as a SPAN or RSPAN destination. You can enable IEEE 802.1x on a SPAN or RSPAN source port.

To globally disable IEEE 802.1x on the switch, use the **no dot1x system-auth-control** global configuration command. To disable IEEE 802.1x on a specific port, use the **no dot1x port-control** interface configuration command.

## Examples

This example shows how to enable IEEE 802.1x on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# dot1x port-control auto
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x re-authenticate

Use the **dot1x re-authenticate** privileged EXEC command to manually initiate a re-authentication of the specified IEEE 802.1x-enabled port.

**dot1x re-authenticate interface** *interface-id*

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | Module and port number of the interface to re-authenticate. |

## Defaults

There is no default setting.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can use this command to re-authenticate a client without waiting for the configured number of seconds between re-authentication attempts (re-authperiod) and automatic re-authentication.

## Examples

This example shows how to manually re-authenticate the device connected to a port:

```
Switch# dot1x re-authenticate interface gigabitethernet0/1
```

# dot1x reauthentication

Use the **dot1x reauthentication** interface configuration command to enable periodic re-authentication of the client. Use the **no** form of this command to return to the default setting.

**dot1x reauthentication**

**no dot1x reauthentication**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Periodic re-authentication is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You configure the amount of time between periodic re-authentication attempts by using the **dot1x timeout reauth-period** interface configuration command.

## Examples

This example shows how to disable periodic re-authentication of the client:

```
Switch(config-if)# no dot1x reauthentication
```

This example shows how to enable periodic re-authentication and to set the number of seconds between re-authentication attempts to 4000 seconds:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x timeout reauth-period** | Sets the number of seconds between re-authentication attempts. |
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x system-auth-control

Use the **dot1x system-auth-control** global configuration command to globally enable IEEE 802.1x. Use the **no** form of this command to return to the default setting.

**dot1x system-auth-control**

**no dot1x system-auth-control**

## Syntax Description

This command has no arguments or keywords.

## Defaults

IEEE 802.1x is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You must enable authentication, authorization, and accounting (AAA) and specify the authentication method list before globally enabling IEEE 802.1x. A method list describes the sequence and authentication methods to be queried to authenticate a user.

Before globally enabling IEEE 802.1x on a switch, remove the EtherChannel configuration from the interfaces on which IEEE 802.1x and EtherChannel are configured.

## Examples

This example shows how to globally enable IEEE 802.1x on a switch:

```
Switch(config)# dot1x system-auth-control
```

You can verify your settings by entering the **show dot1x** [**interface** *interface-id*] privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x port-control** | Enables manual control of the authorization state of the port. |
| **show dot1x** [**interface** *interface-id*] | Displays IEEE 802.1x status for the specified port. |

# dot1x test eapol-capable

Use the **dot1x test eapol-capable** privileged EXEC command to monitor IEEE 802.1x activity on all the switch ports and to display information about the devices that are connected to the ports that support IEEE 802.1x.

**dot1x test eapol-capable** [**interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Port to be queried. |

## Defaults

There is no default setting.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

Use this command to test the IEEE 802.1x capability of the devices connected to all ports or to specific ports on a switch.

There is not a **no** form of this command.

## Examples

This example shows how to enable the IEEE 802.1x readiness check on a switch to query a port. It also shows the response received from the queried port verifying that the device connected to it is IEEE 802.1x-capable:

```
switch# dot1x test eapol-capable interface gigabitethernet1/0/13

DOT1X_PORT_EAPOL_CAPABLE:DOT1X: MAC 00-01-02-4b-f1-a3 on gigabitethernet1/0/13 is EAPOL
capable
```

## Related Commands

| Command | Description |
|---|---|
| **dot1x test timeout** *timeout* | Configures the timeout used to wait for EAPOL response to an IEEE 802.1x readiness query. |

# dot1x test timeout

Use the **dot1x test timeout** global configuration command to configure the timeout used to wait for EAPOL response from a port being queried for IEEE 802.1x readiness.

**dot1x test timeout** *timeout*

## Syntax Description

| | |
|---|---|
| *timeout* | Time in seconds to wait for an EAPOL response. The range is from 1 to 65535 seconds. |

## Defaults

The default setting is 10 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

Use this command to configure the timeout used to wait for EAPOL response.

There is not a **no** form of this command.

## Examples

This example shows how to configure the switch to wait 27 seconds for an EAPOL response:

```
Switch# dot1x test timeout 27
```

You can verify the timeout configuration status by entering the **show run** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x test eapol-capable** [**interface** *interface-id*] | Checks for IEEE 802.1x readiness on devices connected to all or to specified IEEE 802.1x-capable ports. |

# dot1x timeout

Use the **dot1x timeout** interface configuration command to set IEEE 802.1x timers. Use the **no** form of this command to return to the default setting.

**dot1x timeout** {**quiet-period** *seconds* | **reauth-period** *seconds* | **server-timeout** *seconds* | **supp-timeout** *seconds* | **tx-period** *seconds*}

**no dot1x timeout** {**quiet-period** | **reauth-period** | **server-timeout** | **supp-timeout** | **tx-period**}

## Syntax Description

| | |
|---|---|
| **quiet-period** *seconds* | Number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The range is 1 to 65535. |
| **reauth-period** *seconds* | Number of seconds between re-authentication attempts. The range is 1 to 65535. |
| **server-timeout** *seconds* | Number of seconds that the switch waits for the retransmission of packets by the switch to the authentication server. The range is 30 to 65535. |
| **supp-timeout** *seconds* | Number of seconds that the switch waits for the retransmission of packets by the switch to the IEEE 802.1x client. The range is 30 to 65535. |
| **tx-period** *seconds* | Number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The range is 1 to 65535. |

## Defaults

These are the default settings:

**reauth-period** is 3600 seconds.

**quiet-period** is 60 seconds.

**tx-period** is 30 seconds.

**supp-timeout** is 30 seconds.

**server-timeout** is 30 seconds.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(40)SE | The range for **tx-period** seconds is incorrect. The correct range is from 1 to 65535. |

## Usage Guidelines

You should change the default value of this command only to adjust for unusual circumstances such as unreliable links or specific behavioral problems with certain clients and authentication servers.

The **dot1x timeout reauth-period** interface configuration command affects the behavior of the switch only if you have enabled periodic re-authentication by using the **dot1x reauthentication** interface configuration command.

During the quiet period, the switch does not accept or initiate any authentication requests. If you want to provide a faster response time to the user, enter a number smaller than the default.

## Examples

This example shows how to enable periodic re-authentication and to set 4000 as the number of seconds between re-authentication attempts:

```
Switch(config-if)# dot1x reauthentication
Switch(config-if)# dot1x timeout reauth-period 4000
```

This example shows how to set 30 seconds as the quiet time on the switch:

```
Switch(config-if)# dot1x timeout quiet-period 30
```

This example shows how to set 45 seconds as the switch-to-authentication server retransmission time:

```
Switch(config)# dot1x timeout server-timeout 45
```

This example shows how to set 45 seconds as the switch-to-client retransmission time for the EAP request frame:

```
Switch(config-if)# dot1x timeout supp-timeout 45
```

This example shows how to set 60 as the number of seconds to wait for a response to an EAP-request/identity frame from the client before re-transmitting the request:

```
Switch(config-if)# dot1x timeout tx-period 60
```

You can verify your settings by entering the **show dot1x** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **dot1x max-req** | Sets the maximum number of times that the switch sends an EAP-request/identity frame before restarting the authentication process. |
| **dot1x reauthentication** | Enables periodic re-authentication of the client. |
| **show dot1x** | Displays IEEE 802.1x status for all ports. |

# duplex

Use the **duplex** interface configuration command to specify the duplex mode of operation for a port. Use the **no** form of this command to return the port to its default value.

**duplex** {**auto** | **full** | **half**}

**no duplex**

## Syntax Description

| | |
|---|---|
| **auto** | Enable automatic duplex configuration; port automatically detects whether it should run in full- or half-duplex mode, depending on the attached device mode. |
| **full** | Enable full-duplex mode. |
| **half** | Enable half-duplex mode (only for interfaces operating at 10 Mbps or 100 Mbps). You cannot configure half-duplex mode for interfaces operating at 1000 Mbps or 10,000 Mbps. |

## Defaults

The default is **auto** for Fast Ethernet and Gigabit Ethernet ports and for 1000BASE-T small form-factor pluggable (SFP) modules.

The default is **half** for 100BASE-FX MMF SFP modules.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This command is only available when a 1000BASE-T SFP module or a 100BASE-FX MMF SFP module is in the SFP module slot. All other SFP modules operate only in full-duplex mode.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure duplex mode to **auto** or **full**.

When a 100BASE-FX MMF SFP module is in the SFP module slot, you can configure duplex mode to **half** or **full**. Although the **auto** keyword is available, it puts the interface in half-duplex mode (the default) because the 100BASE-FX MMF SFP module does not support autonegotiation.

Certain ports can be configured to be either full duplex or half duplex. Applicability of this command depends on the device to which the switch is attached.

For Fast Ethernet ports, setting the port to **auto** has the same effect as specifying **half** if the attached device does not autonegotiate the duplex parameter.

For Gigabit Ethernet ports, setting the port to **auto** has the same effect as specifying **full** if the attached device does not autonegotiate the duplex parameter.

**Note** Half-duplex mode is supported on Gigabit Ethernet interfaces if duplex mode is **auto** and the connected device is operating at half duplex. However, you cannot configure these interfaces to operate in half-duplex mode.

If both ends of the line support autonegotiation, we highly recommend using the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, configure duplex and speed on both interfaces; do use the **auto** setting on the supported side.

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

You can configure the duplex setting when the speed is set to **auto**.

**Caution** Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

**Note** For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

## Examples

This example shows how to configure an interface for full duplex operation:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# duplex full
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays the interface settings on the switch. |
| **speed** | Sets the speed on a 10/100 or 10/100/1000 Mbps interface. |

# errdisable detect cause

Use the **errdisable detect cause** global configuration command to enable error-disabled detection for a specific cause or all causes. Use the **no** form of this command to disable the error-disabled detection feature.

**errdisable detect cause** {**all** | **dhcp-rate-limit** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap**}

**no errdisable detect cause** {**all** | **dhcp-rate-limit** | **gbic-invalid** | **link-flap** | **pagp-flap**}

## Syntax Description

| | |
|---|---|
| **all** | Enable error detection for all error-disable causes. |
| **dhcp-rate-limit** | Enable error detection for DHCP snooping. |
| **gbic-invalid** | Enable error detection for an invalid Gigabit Interface Converter (GBIC) module.<br>**Note** This error refers to an invalid small form-factor pluggable (SFP) module. |
| **link-flap** | Enable error detection for link-state flapping. |
| **loopback** | Enable error detection for detected loopbacks. |
| **pagp-flap** | Enable error detection for the Port Aggregation Protocol (PAgP) flap error-disabled cause. |

**Note** Though visible in the command-line help string, the **arp-inspection** keyword is not supported.

## Defaults

Detection is enabled for all causes. All causes, except for per-VLAN error disabling**,** are configured to shut down the entire port.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A cause (**all**, **dhcp-rate-limit**, and so forth) is the reason why the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in an error-disabled state, an operational state that is similar to a link-down state.

When a port is error-disabled, it is effectively shut down, and no traffic is sent or received on the port. For the BPDU guard and port-security features, you can configure the switch to shut down just the offending VLAN on the port when a violation occurs, instead of shutting down the entire port.

If you set a recovery mechanism for the cause by entering the **errdisable recovery** global configuration command for the cause, the interface is brought out of the error-disabled state and allowed to retry the operation when all causes have timed out. If you do not set a recovery mechanism, you must enter the **shutdown** and then the **no shutdown** commands to manually recover an interface from the error-disabled state.

## Examples

This example shows how to enable error-disabled detection for the link-flap error-disabled cause:

```
Switch(config)# errdisable detect cause link-flap
```

You can verify your setting by entering the **show errdisable detect** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show errdisable detect** | Displays errdisable detection information. |
| **show interfaces status err-disabled** | Displays interface status or a list of interfaces in the error-disabled state. |

# errdisable detect cause small-frame

Use the **errdisable detect cause small-frame** global configuration command on the switch stack or on a standalone switch to allow any switch port to be error disabled if incoming VLAN-tagged packets are small frames (67 bytes or less) and arrive at the minimum configured rate (the threshold). Use the **no** form of this command to return to the default setting.

**errdisable detect cause small-frame**

**no** errdisable detect cause small-frame

## Syntax Description

This command has no arguments or keywords.

## Defaults

This feature is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

This command globally enables the small-frame arrival feature. Use the **small violation-rate** interface configuration command to set the threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** *interval global configuration command.*

## Examples

This example shows how to enable the switch ports to be put into the error-disabled mode if incoming small frames arrive at the configured threshold:

```
Switch(config)# errdisable detect cause small-frame
```

You can verify your setting by entering the **show interfaces** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **errdisable recovery cause small-frame** | Enables the recovery timer. |
| **errdisable recovery interval** *interval* | Specifies the time to recover from the specified error-disabled state. |

| Command | Description |
|---|---|
| **show interfaces** | Displays the interface settings on the switch, including input and output flow control. |
| **small-frame violation-rate** | Configures the rate (threshold) for incoming small frames to cause a port to be put into the error-disabled state. |

# errdisable recovery cause small-frame

Use the **errdisable recovery cause small-frame** global configuration command on the switch stack or on a standalone switch to enable the recovery timer for ports to be automatically re-enabled after they are error disabled by the arrival of small frames. Use the **no** form of this command to return to the default setting.

**errdisable recovery cause small-frame**

**no errdisable recovery cause small-frame**

## SyntaxDescription

This command has no arguments or keywords.

## Defaults

This feature is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

This command enables the recovery timer for error-disabled ports. You configure the recovery time by using the errdisable **recovery interval** *interval interface configuration command.*

## Examples

This example shows how to set the recovery timer:

```
Switch(config)# errdisable recovery cause small-frame
```

You can verify your setting by entering the **show interfaces** user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **errdisable detect cause small-frame** | Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the configured minimum size and arrives at the specified rate (threshold). |
| **show interfaces** | Displays the interface settings on the switch, including input and output flow control. |
| **small-frame violation-rate** | Configures the size for an incoming (small) frame to cause a port to be put into the error-disabled state. |

# errdisable recovery

Use the **errdisable recovery** global configuration command to configure the recover mechanism variables. Use the **no** form of this command to return to the default setting.

**errdisable recovery** {**cause** {**all** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **udld** |**unicast-flood** | **vmps**} | {**interval** *interval*}

**no errdisable recovery** {**cause** {**all** | **bpduguard** | **channel-misconfig** | **dhcp-rate-limit** | **gbic-invalid** | **link-flap** | **loopback** | **pagp-flap** | **psecure-violation** | **security-violation** | **udld** |**unicast-flood** | **vmps**} | {**interval** *interval*}

## Syntax Description

| | |
|---|---|
| **cause** | Enable the error-disabled mechanism to recover from a specific cause. |
| **all** | Enable the timer to recover from all error-disabled causes. |
| **bpduguard** | Enable the timer to recover from the bridge protocol data unit (BPDU) guard error-disabled state. |
| **channel-misconfig** | Enable the timer to recover from the EtherChannel misconfiguration error-disabled state. |
| **dhcp-rate-limit** | Enable the timer to recover from the DHCP snooping error-disabled state. |
| **gbic-invalid** | Enable the timer to recover from an invalid Gigabit Interface Converter (GBIC) module error-disable state.<br>**Note** This error refers to an invalid small form-factor pluggable (SFP) error-disable state. |
| **link-flap** | Enable the timer to recover from the link-flap error-disabled state. |
| **loopback** | Enable the timer to recover from a loopback error-disabled state. |
| **pagp-flap** | Enable the timer to recover from the Port Aggregation Protocol (PAgP)-flap error-disabled state. |
| **psecure-violation** | Enable the timer to recover from a port security violation disable state. |
| **security-violation** | Enable the timer to recover from an IEEE 802.1x-violation disabled state |
| **udld** | Enable the timer to recover from the UniDirectional Link Detection (UDLD) error-disabled state. |
| **unicast-flood** | Enable the timer to recover from the unicast flood disable state. |
| **vmps** | Enable the timer to recover from the VLAN Membership Policy Server (VMPS) error-disabled state. |
| **interval** *interval* | Specify the time to recover from the specified error-disabled state. The range is 30 to 86400 seconds. The same interval is applied to all causes. The default interval is 300 seconds.<br>**Note** The error-disabled recovery timer is initialized at a random differential from the configured interval value. The difference between the actual timeout value and the configured value can be up to 15 percent of the configured interval. |

**Note** Though visible in the command-line help strings, the **arp-inspection**, **storm-control**, and **unicast-flood** keywords are not supported.

## Defaults

Recovery is disabled for all causes.

The default recovery interval is 300 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A cause (**all**, **bpduguard** and so forth) is defined as the reason that the error-disabled state occurred. When a cause is detected on an interface, the interface is placed in error-disabled state, an operational state similar to link-down state. If you do not enable errdisable recovery for the cause, the interface stays in error-disabled state until you enter a **shutdown** and **no shutdown** interface configuration command. If you enable the recovery for a cause, the interface is brought out of the error-disabled state and allowed to retry the operation again when all the causes have timed out.

Otherwise, you must enter the **shutdown** then **no shutdown** commands to manually recover an interface from the error-disabled state

## Examples

This example shows how to enable the recovery timer for the BPDU guard error-disabled cause:

```
Switch(config)# errdisable recovery cause bpduguard
```

This example shows how to set the timer to 500 seconds:

```
Switch(config)# errdisable recovery interval 500
```

You can verify your settings by entering the **show errdisable recovery** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show errdisable recovery** | Displays errdisable recovery timer information. |
| **show interfaces status err-disabled** | Displays interface status or a list of interfaces in error-disabled state. |

# exceed-action

Use the **exceed-action** policy-map class police configuration command to set multiple actions for a policy-map class for packets that do not conform to the committed information rate (CIR). Use the **no** form of this command to cancel the action or return to the default action.

**exceed-action** {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

**no exceed-action** {**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]}

## Syntax Description

| | |
|---|---|
| **drop** | Drop the packet. |
| **set-cos-transmit** *new-cos-value* | Set a new class of service (CoS) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new CoS value is 0 to 7. |
| **set-dscp-transmit** *new-dscp-value* | Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new DCSP value is 0 to 63. |
| **set-prec-transmit** *new-precedence-value* | Set a new IP precedence value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new IP precedence value is 0 to 7. |
| **set-qos-transmit** *qos-group-value* | Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new QoS value is 0 to 99. |
| **cos** | (Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **dscp** | (Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **precedence** | (Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **table** *table-map name* | (Optional) Used in conjunction with the preceding *from-type* keyword. Specify the table map to be used for the enhanced packet marking. The *to-type* of the action is marked based on the *from-type* parameter of the action using this table map. |
| **transmit** | (Optional) Send the packet unmodified. |

## Defaults

The default action is to drop the packet.

**Command Modes**

Policy-map class police configuration

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Increased support for configuring exceed actions. See "Usage Guidelines." |

**Usage Guidelines**

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.

Access policy-map class police configuration mode by entering the **police** policy-map class command. See the **police** command for more information.

You can use this command to set one or more exceed actions for a traffic class.

**Examples**

This example shows how configure multiple actions in a policy map that sets an information rate of 23000 bits per second (bps) and a burst rate of 10000 bps:

```
Switch(config)# policy-map map1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 23000 10000
Switch(config-pmap-c-police)# conform-action transmit
Switch(config-pmap-c-police)# exceed-action set-prec-transmit prec table
policed-prec-table-map-name
Switch(config-pmap-c-police)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **conform-action** | Defines the action to take on traffic that conforms to the CIR. |
| **police** | Defines a policer for classified traffic. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |

# flowcontrol

Use the **flowcontrol** interface configuration command to set the receive flow-control state for an interface. When flow control **send** is operable and on for a device and it detects any congestion at its end, it notifies the link partner or the remote device of the congestion by sending a pause frame. When flow control **receive** is on for a device and it receives a pause frame, it stops sending any data packets. This prevents any loss of data packets during the congestion period.

Use the **receive off** keywords to disable flow control.

**flowcontrol receive** {**desired** | **off** | **on**}

**Note** The Cisco ME switch can only receive pause frames.

## Syntax Description

| | |
|---|---|
| **receive** | Set whether the interface can receive flow-control packets from a remote device. |
| **desired** | Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets. |
| **off** | Turn off the ability of an attached device to send flow-control packets to an interface. |
| **on** | Allow an interface to operate with an attached device that is required to send flow-control packets or with an attached device that is not required to but can send flow-control packets. |

## Defaults

The default is **flowcontrol receive off**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switch does not support sending flow-control pause frames. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **flowcontrol** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

Note that the **on** and **desired** keywords have the same result.

When you use the **flowcontrol** command to set a port to control traffic rates during congestion, you are setting flow control on a port to one of these conditions:

- **receive on** or **desired**: The port cannot send out pause frames, but can operate with an attached device that is required to or is able to send pause frames; the port is able to receive pause frames.
- **receive off**: Flow control does not operate in either direction. In case of congestion, no indication is given to the link partner and no pause frames are sent or received by either device.

Table 2-2 shows the flow control results on local and remote ports for a combination of settings. The table assumes that **receive desired** has the same results as using the **receive on** keywords.

*Table 2-2 Flow Control Settings and Local and Remote Port Flow Control Resolution*

| Flow Control Settings | | Flow Control Resolution | |
|---|---|---|---|
| **Local Device** | **Remote Device** | **Local Device** | **Remote Device** |
| **send off/receive on** | **send on/receive on** | Receives only | Sends and receives |
| | **send on/receive off** | Receives only | Sends only |
| | **send desired/receive on** | Receives only | Sends and receives |
| | **send desired/receive off** | Receives only | Sends only |
| | **send off/receive on** | Receives only | Receives only |
| | **send off/receive off** | Does not send or receive | Does not send or receive |
| **send off/receive off** | **send on/receive on** | Does not send or receive | Does not send or receive |
| | **send on/receive off** | Does not send or receive | Does not send or receive |
| | **send desired/receive on** | Does not send or receive | Does not send or receive |
| | **send desired/receive off** | Does not send or receive | Does not send or receive |
| | **send off/receive on** | Does not send or receive | Does not send or receive |
| | **send off/receive off** | Does not send or receive | Does not send or receive |

## Examples

This example shows how to configure the local port to not support flow control by the remote port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# flowcontrol receive off
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays the interface settings on the switch, including input and output flow control. |

# interface port-channel

Use the **interface port-channel** global configuration command to access or create the port-channel logical interface. Use the **no** form of this command to remove the port-channel.

**interface port-channel** *port-channel-number*

**no interface port-channel** *port-channel-number*

## Syntax Description

| | |
|---|---|
| *port-channel-number* | Port-channel number. The range is 1 to 48. |

## Defaults

No port-channel logical interfaces are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For Layer 2 EtherChannels, you do not have to create a port-channel interface first before assigning a physical port to a channel group. Instead, you can use the **channel-group** interface configuration command. It automatically creates the port-channel interface when the channel group gets its first physical port. If you create the port-channel interface first, the *channel-group-number* can be the same as the *port-channel-number,* or you can use a new number. If you use a new number, the **channel-group** command dynamically creates a new port channel.

Only one port channel in a channel group is allowed.

Follow these guidelines when you use the **interface port-channel** command:

- If you want to use the Cisco Discovery Protocol (CDP), you must configure it only on the physical port and not on the port-channel interface.

**Note** CDP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

- Do not configure a port that is an active member of an EtherChannel as an IEEE 802.1x port. If IEEE 802.1x is enabled on a not-yet active port of an EtherChannel, the port does not join the EtherChannel.

For a complete list of configuration guidelines, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

## Examples

This example shows how to create a port-channel interface with a port channel number of 5:

```
Switch(config)# interface port-channel 5
```

You can verify your setting by entering the **show running-config** privileged EXEC or **show etherchannel** *channel-group-number* **detail** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns an Ethernet port to an EtherChannel group. |
| **show etherchannel** | Displays EtherChannel information for a channel. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# interface range

Use the **interface range** global configuration command to enter interface range configuration mode and to execute a command on multiple ports at the same time. Use the **no** form of this command to remove an interface range.

**interface range** {*port-range* | **macro** *name*}

**no interface range** {*port-range* | **macro** *name*}

## Syntax Description

| | |
|---|---|
| *port-range* | Port range. For a list of valid values for *port-range*, see the "Usage Guidelines" section. |
| **macro** *name* | Specify the name of a macro. |

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you enter interface range configuration mode, all interface parameters you enter are attributed to all interfaces within the range.

For VLANs, you can use the **interface range** command only on existing VLAN switch virtual interfaces (SVIs). To display VLAN SVIs, enter the **show running-config** privileged EXEC command. VLANs not displayed cannot be used in the **interface range** command. The commands entered under **interface range** command are applied to all existing VLAN SVIs in the range.

All configuration changes made to an interface range are saved to NVRAM, but the interface range itself is not saved to NVRAM.

You can enter the interface range in two ways:

- Specifying up to five interface ranges
- Specifying a previously defined interface-range macro

All interfaces in a range must be the same type; that is, all Fast Ethernet ports, all Gigabit Ethernet ports, all EtherChannel ports, or all VLANs. However, you can define up to five interface ranges with a single command, with each range separated by a comma.

Valid values for *port-range* type and interface:

- **vlan** *vlan-ID - vlan-ID*, where VLAN ID is from 1 to 4094
- **fastethernet module/**{*first port*} - {*last port*}, where module is always **0**
- **gigabitethernet** *module/*{*first port*} - {*last port*}, where module is always **0**

  For physical interfaces:

  – module is always 0

  – the range is *type* **0/***number - number* (for example, **gigabitethernet0/1 - 2**)
- **port-channel** *port-channel-number - port-channel-number*, where *port-channel-number* is from 1 to 48

**Note** When you use the **interface range** command with port channels, the first and last port channel number in the range must be active port channels.

When you define a range, you must enter a space between the first entry and the hyphen (-):

```
interface range gigabitethernet0/1 -2
```

When you define multiple ranges, you must still enter a space after the first entry and before the comma (,):

```
interface range fastethernet0/1 - 2, gigabitethernet0/1 - 2
```

You cannot specify both a macro and an interface range in the same command.

A single interface can also be specified in *port-range* (this would make the command similar to the **interface** *interface-id* global configuration command).

**Note** For more information about configuring interface ranges, see the software configuration guide for this release.

## Examples

This example shows how to use the **interface range** command to enter interface range configuration mode to apply commands to two ports:

```
Switch(config)# interface range gigabitethernet0/1 - 2
Switch(config-if-range)#
```

This example shows how to use a port-range macro *macro1* for the same function. The advantage is that you can reuse *macro1* until you delete it.

```
Switch(config)# define interface-range macro1 gigabitethernet0/1 - 2
Switch(config)# interface range macro macro1
Switch(config-if-range)#
```

## Related Commands

| Command | Description |
|---|---|
| **define interface-range** | Creates an interface range macro. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# interface vlan

Use the **interface vlan** global configuration command to create or access a VLAN and to enter interface configuration mode. Use the **no** form of this command to delete a VLAN.

**interface vlan** *vlan-id*

**no interface vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN number. The range is 1 to 4094. |

## Defaults

The default VLAN interface is VLAN 1.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2.(25)EX | This command was introduced. |

## Usage Guidelines

VLANs are created the first time that you enter the **interface vlan** *vlan-id* command for a particular *vlan*. The *vlan-id* corresponds to the VLAN-tag associated with data frames on an IEEE 802.1Q encapsulated trunk or the VLAN ID configured for an access port.

If you delete a VLAN by entering the **no interface vlan** *vlan-id* command, the deleted interface is no longer visible in the output from the **show interfaces** privileged EXEC command.

**Note** You cannot delete the VLAN 1 interface.

You can reinstate a deleted VLAN by entering the **interface vlan** *vlan-id* command for the deleted interface. The interface comes back up, but much of the previous configuration will be gone.

## Examples

This example shows how to create a new VLAN with VLAN ID 23 and enter interface configuration mode:

```
Switch(config)# interface vlan 23
Switch(config-if)#
```

You can verify your setting by entering the **show interfaces** and **show interfaces vlan** *vlan-id* privileged EXEC commands.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces vlan** *vlan-id* | Displays the administrative and operational status of all interfaces or the specified VLAN. |

# ip access-group

Use the **ip access-group** interface configuration command to control access to a Layer 2 interface. Use the **no** form of this command to remove all access groups or the specified access group from the interface.

**ip access-group** {*access-list-number* | *name*} {**in**}

**no ip access-group** [*access-list-number* | *name*] {**in**}

## Syntax Description

| | |
|---|---|
| *access-list-number* | The number of the IP access control list (ACL). The range is 1 to 199 or 1300 to 2699. |
| *name* | The name of an IP ACL, specified in the **ip access-list** global configuration command. |
| **in** | Specify filtering on inbound packets. |

## Defaults

No access list is applied to the interface.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can apply named or numbered standard or extended IP access lists to an interface. To define an access list by name, use the **ip access-list** global configuration command. To define a numbered access list, use the **access list** global configuration command. You can used numbered standard access lists ranging from 1 to 99 and 1300 to 1999 or extended access lists ranging from 100 to 199 and 2000 to 2699.

You can use this command to apply an access list to a Layer 2 interface. However, note these limitations for port ACLs:

- You can only apply ACLs in the inbound direction.
- You can only apply one IP ACL and one MAC ACL per interface.
- Port ACLs do not support logging; if the **log** keyword is specified in the IP ACL, it is ignored.
- An IP ACL applied to an interface only filters IP packets. To filter non-IP packets, use the **mac access-group** interface configuration command with MAC extended ACLs.

You can use input port ACLs and VLAN maps on the same switch. However, a port ACL takes precedence over a VLAN map. When both an input port ACL and a VLAN map are applied, incoming packets received on ports with the port ACL applied are filtered by the port ACL. Other packets are filtered by the VLAN map.

For standard inbound access lists, after the switch receives a packet, it checks the source address of the packet against the access list. IP extended access lists can optionally check other fields in the packet, such as the destination IP address, protocol type, or port numbers. If the access list permits the packet, the switch continues to process the packet. If the access list denies the packet, the switch discards the packet.

If the specified access list does not exist, all packets are passed.

## Examples

This example shows how to apply IP access list 101 to inbound packets on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip access-group 101 in
```

You can verify your settings by entering the **show ip interface, show access-lists,** or **show ip access-lists** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **access list** | Configures a numbered ACL. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands** |
| **ip access-list** | Configures a named ACL. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.** |
| **show access-lists** | Displays ACLs configured on the switch. |
| **show ip interface** | Displays information about interface status and configuration. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**. |

# ip address

Use the **ip address** interface configuration command to set an IP address for the Layer 2 switch. Use the **no** form of this command to remove an IP address or to disable IP processing.

**ip address** *ip-address subnet-mask* [**secondary**]

**no ip address** [*ip-address subnet-mask*] [**secondary**]

## Syntax Description

| | |
|---|---|
| *ip-address* | IP address. |
| *subnet-mask* | Mask for the associated IP subnet. |
| **secondary** | (Optional) Specifies that the configured address is a secondary IP address. If this keyword is omitted, the configured address is the primary IP address. |

## Defaults

No IP address is defined.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12,2(25)EX | This command was introduced. |

## Usage Guidelines

If you remove the switch IP address through a Telnet session, your connection to the switch will be lost.

Hosts can find subnet masks using the Internet Control Message Protocol (ICMP) Mask Request message. Routers respond to this request with an ICMP Mask Reply message.

You can disable IP processing on a particular interface by removing its IP address with the **no ip address** command. If the switch detects another host using one of its IP addresses, it will send an error message to the console.

You can use the optional keyword **secondary** to specify an unlimited number of secondary addresses. Secondary addresses are treated like primary addresses, except the system never generates datagrams other than routing updates with secondary source addresses. IP broadcasts and ARP requests are handled properly, as are interface routes in the IP routing table.

**Note** If any router on a network segment uses a secondary address, all other devices on that same segment must also use a secondary address from the same network or subnet. Inconsistent use of secondary addresses on a network segment can very quickly cause routing loops.

If your switch receives its IP address from a Bootstrap Protocol (BOOTP) or a DHCP server and you remove the switch IP address by using the **no ip address** command, IP processing is disabled, and the BOOTP or the DHCP server cannot reassign the address.

## Examples

This example shows how to configure the IP address for the Layer 2 switch on a subnetted network:

```
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.20.128.2 255.255.255.0
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# ip dhcp snooping

Use the **ip dhcp snooping** global configuration command to globally enable DHCP snooping. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping**

**no ip dhcp snooping**

## Syntax Description

This command has no arguments or keywords.

## Defaults

DHCP snooping is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For any DHCP snooping configuration to take effect, you must globally enable DHCP snooping.

DHCP snooping is not active until you enable snooping on a VLAN by using the **ip dhcp snooping vlan** *vlan-id* global configuration command.

## Examples

This example shows how to enable DHCP snooping:

```
Switch(config)# ip dhcp snooping
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping vlan** | Enables DHCP snooping on a VLAN. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# ip dhcp snooping binding

Use the **ip dhcp snooping binding** privileged EXEC command to configure the DHCP snooping binding database and to add binding entries to the database. Use the **no** form of this command to delete entries from the binding database.

**ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id* **expiry** *seconds*

**no ip dhcp snooping binding** *mac-address* **vlan** *vlan-id ip-address* **interface** *interface-id*

## Syntax Description

| | |
|---|---|
| *mac-address* | Specify a MAC address. |
| **vlan** *vlan-id* | Specify a VLAN number. The range is from 1 to 4904. |
| *ip-address* | Specify an IP address. |
| **interface** *interface-id* | Specify an interface on which to add or delete a binding entry. |
| **expiry** *seconds* | Specify the interval (in seconds) after which the binding entry is no longer valid. The range is from 1 to 4294967295. |

## Defaults

No default database is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command when you are testing or debugging the switch.

In the DHCP snooping binding database, each database entry, also referred to a binding, has an IP address, an associated MAC address, the lease time (in hexadecimal format), the interface to which the binding applies, and the VLAN to which the interface belongs. The database can have up to 8192 bindings.

Use the **show ip dhcp snooping binding** privileged EXEC command to display only the dynamically configured bindings. Use the **show ip source binding** privileged EXEC command to display the dynamically and statically configured bindings.

## Examples

This example shows how to generate a DHCP binding configuration with an expiration time of 1000 seconds on a port in VLAN 1:

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface
gigabitethernet0/1 expiry 1000
```

You can verify your settings by entering the **show ip dhcp snooping binding** or the **show ip dhcp source binding** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables DHCP snooping on a VLAN. |
| **show ip dhcp snooping binding** | Displays the dynamically configured bindings in the DHCP snooping binding database and the configuration information. |

# ip dhcp snooping database

Use the **ip dhcp snooping database** global configuration command to configure the DHCP snooping binding database agent. Use the **no** form of this command to disable the agent, to reset the timeout value, or to reset the write-delay value.

**ip dhcp snooping database {{flash:/***filename* **| ftp://***user:password@host/filename* **| http://***[[username:password]@]{hostname | host-ip}[/directory]/image-name***.tar | rcp://***user@host/filename* **| tftp://***host/filename***} | timeout** *seconds* **| write-delay** *seconds***}**

**no ip dhcp snooping database** [**timeout | write-delay**]

## Syntax Description

| | |
|---|---|
| **flash:/***filename* | Specify that the database agent or the binding file is in the flash memory. |
| **ftp://***user***:***password@host/filename* | Specify that the database agent or the binding file is on an FTP server. |
| **http://***[[username:password]@] {hostname \| host-ip}[/directory] /image-name***.tar** | Specify that the database agent or the binding file is on an FTP server. |
| **rcp://***user@host/filename* | Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server. |
| **tftp://***host/filename* | Specify that the database agent or the binding file is on a TFTP server. |
| **timeout** *seconds* | Specify (in seconds) when to stop the database transfer process after the DHCP snooping binding database changes.<br>The default is 300 seconds. The range is from 0 to 86400. Use 0 to define an infinite duration. |
| **write-delay** *seconds* | Specify (in seconds) the duration for which the transfer should be delayed after the binding database changes. The default is 300 seconds. The range is from 15 to 86400. |

## Defaults

The URL for the database agent or binding file is not defined.

The timeout value is 300 seconds (5 minutes).

The write-delay value is 300 seconds (5 minutes).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The DHCP snooping binding database can have up to 8192 bindings.

To ensure that the lease time in the database is accurate, we recommend that Network Time Protocol (NTP) is enabled and configured for these features:

- NTP authentication
- NTP peer and server associations
- NTP broadcast service
- NTP access restrictions
- NTP packet source IP address

If NTP is configured, the switch writes binding changes to the binding file only when the switch system clock is synchronized with NTP.

Because both NVRAM and the flash memory have limited storage capacity, we recommend that you store a binding file on a TFTP server. You must create an empty file at the configured URL on network-based URLs (such as TFTP and FTP) before the switch can write bindings to the binding file at that URL for the first time.

Use the **no ip dhcp snooping database** command to disable the agent.

Use the **no ip dhcp snooping database timeout** command to reset the timeout value.

Use the **no ip dhcp snooping database write-delay** command to reset the write-delay value.

## Examples

This example shows how to store a binding file at an IP address of 10.1.1.1 that is in a directory called *directory*. A file named *file* must be present on the TFTP server.

```
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
```

You can verify your settings by entering the **show ip dhcp snooping database** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| ip dhcp snooping | Enables DHCP snooping on a VLAN. |
| ip dhcp snooping binding | Configures the DHCP snooping binding database. |
| show ip dhcp snooping database | Displays the status of DHCP snooping database agent. |

# ip dhcp snooping information option

Use the **ip dhcp snooping information option** global configuration command to enable DHCP option-82 data insertion. Use the **no** form of this command to disable DHCP option-82 data insertion.

**ip dhcp snooping information option**

**no ip dhcp snooping information option**

## Syntax Description

This command has no arguments or keywords.

## Defaults

DHCP option-82 data insertion is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled and a switch receives a DHCP request from a host, it adds the option-82 information in the packet. The option-82 information contains the switch MAC address (the remote ID suboption) and the port identifier, **vlan-mod-port**, from which the packet is received (circuit ID suboption). The switch forwards the DHCP request that includes the option-82 field to the DHCP server.

When the DHCP server receives the packet, it can use the remote ID, the circuit ID, or both to assign IP addresses and implement policies, such as restricting the number of IP addresses that can be assigned to a single remote ID or a circuit ID. Then the DHCP server echoes the option-82 field in the DHCP reply.

The DHCP server unicasts the reply to the switch if the request was relayed to the server by the switch. When the client and server are on the same subnet, the server broadcasts the reply. The switch inspects the remote ID and possibly the circuit ID fields to verify that it originally inserted the option-82 data. The switch removes the option-82 field and forwards the packet to the switch port that connects to the DHCP host that sent the DHCP request.

## Examples

This example shows how to enable DHCP option-82 data insertion:

```
Switch(config)# ip dhcp snooping information option
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# ip dhcp snooping information option allowed-untrusted

Use the **ip dhcp snooping information option allowed-untrusted** global configuration command on an aggregation switch to configure it to accept DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch. Use the **no** form of this command to configure the switch to drop these packets from the edge switch.

**ip dhcp snooping information option allowed-untrusted**

**no ip dhcp snooping information option allowed-untrusted**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The switch drops DHCP packets with option-82 information that are received on untrusted ports that might be connected to an edge switch.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You might want an edge switch to which a host is connected to insert DHCP option-82 information at the edge of your network. You might also want to enable DHCP security features, such as DHCP snooping, IP source guard, or dynamic Address Resolution Protocol (ARP) inspection, on an aggregation switch. However, if DHCP snooping is enabled on the aggregation switch, the switch drops packets with option-82 information that are received on an untrusted port and does not learn DHCP snooping bindings for connected devices on a trusted interface.

If the edge switch to which a host is connected inserts option-82 information and you want to use DHCP snooping on an aggregation switch, enter the **ip dhcp snooping information option allowed-untrusted** command on the aggregation switch. The aggregation switch can learn the bindings for a host even though the aggregation switch receives DHCP snooping packets on an untrusted port. You can also enable DHCP security features on the aggregation switch. The port on the edge switch to which the aggregation switch is connected must be configured as a trusted port.

**Note** Do not enter the **ip dhcp snooping information option allowed-untrusted** command on an aggregation switch to which an untrusted device is connected. If you enter this command, an untrusted device might spoof the option-82 information.

## Examples

This example shows how to configure an access switch to not check the option-82 information in untrusted packets from an edge switch and to accept the packets:

```
Switch(config)# ip dhcp snooping information option allowed-untrusted
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# ip dhcp snooping information option format remote-id

Use the **ip dhcp snooping information option format remote-id** global configuration command to configure the option-82 remote-ID suboption. Use the **no** form of this command to configure the default remote-ID suboption.

**ip dhcp snooping information option format remote-id** [**string** *ASCII-string* | **hostname**]

**no ip dhcp snooping information option format remote-id**

## Syntax Description

| | |
|---|---|
| **string** *ASCII-string* | Specify a remote ID, using from 1 to 63 ASCII characters (no spaces). |
| **hostname** | Specify the switch hostname as the remote ID. |

## Defaults

The switch MAC address is the remote ID.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SEG | This command was introduced. |

## Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default remote-ID suboption is the switch MAC address. This command allows you to configure either the switch hostname or a string of up to 63 ASCII characters (but no spaces) to be the remote ID.

**Note** If the hostname exceeds 63 characters, it is truncated to 63 characters in the remote-ID configuration.

## Examples

This example shows how to configure the option-82 remote-ID suboption:

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping vlan information option format-type circuit-id string** | Configures the option-82 circuit-ID suboption. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |

# ip dhcp snooping limit rate

Use the **ip dhcp snooping limit rate** interface configuration command to configure the number of DHCP messages an interface can receive per second. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping limit rate** *rate*

**no ip dhcp snooping limit rate**

## Syntax Description

| | |
|---|---|
| *rate* | Number of DHCP messages an interface can receive per second. The range is 1 to 2048. |

## Defaults

DHCP snooping rate limiting is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Normally, the rate limit applies to untrusted interfaces. If you want to configure rate limiting for trusted interfaces, keep in mind that trusted interfaces might aggregate DHCP traffic on multiple VLANs (some of which might not be snooped) in the switch, and you will need to adjust the interface rate limits to a higher value.

If the rate limit is exceeded, the interface is error-disabled. If you enabled error recovery by entering the **errdisable recovery dhcp-rate-limit** global configuration command, the interface retries the operation again when all the causes have timed out. If the error-recovery mechanism is not enabled, the interface stays in the error-disabled state until you enter the **shutdown** and **no shutdown** interface configuration commands.

## Examples

This example shows how to set a message rate limit of 150 messages per second on an interface:

```
Switch(config-if)# ip dhcp snooping limit rate 150
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **errdisable recovery** | Configures the recover mechanism. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# ip dhcp snooping trust

Use the **ip dhcp snooping trust** interface configuration command to configure a port as trusted for DHCP snooping purposes. Use the **no** form of this command to return to the default setting.

**ip dhcp snooping trust**

**no ip dhcp snooping trust**

## Syntax Description

This command has no arguments or keywords.

## Defaults

DHCP snooping trust is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Configure as trusted ports those that are connected to a DHCP server or to other switches or routers. Configure as untrusted ports those that are connected to DHCP clients.

## Examples

This example shows how to enable DHCP snooping trust on a port:

```
Switch(config-if)# ip dhcp snooping trust
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show ip dhcp snooping | Displays the DHCP snooping configuration. |
| show ip dhcp snooping binding | Displays the DHCP snooping binding information. |

# ip dhcp snooping verify mac-address

Use the **ip dhcp snooping verify mac-address** global configuration command to configure the switch to verify on an untrusted port that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to configure the switch to not verify the MAC addresses.

**ip dhcp snooping verify mac-address**

**no ip dhcp snooping verify mac-address**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The switch verifies the source MAC address in a DHCP packet that is received on untrusted ports matches the client hardware address in the packet.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

In a service-provider network, when a switch receives a packet from a DHCP client on an untrusted port, it automatically verifies that the source MAC address and the DHCP client hardware address match. If the addresses match, the switch forwards the packet. If the addresses do not match, the switch drops the packet.

## Examples

This example shows how to disable the MAC address verification:

```
Switch(config)# no ip dhcp snooping verify mac-address
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |

# ip dhcp snooping vlan

Use the **ip dhcp snooping vlan** global configuration command to enable DHCP snooping on a VLAN. Use the **no** form of this command to disable DHCP snooping on a VLAN.

**ip dhcp snooping vlan** *vlan-range*

**no ip dhcp snooping vlan** *vlan-range*

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-range* | Specify a VLAN ID or a range of VLANs on which to enable DHCP snooping. The range is 1 to 4094.<br>You can enter a single VLAN ID identified by VLAN ID number, a series of VLAN IDs separated by commas, a range of VLAN IDs separated by hyphens, or a range of VLAN IDs separated by entering the starting and ending VLAN IDs separated by a space. |

## Defaults

DHCP snooping is disabled on all VLANs.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You must first globally enable DHCP snooping before enabling DHCP snooping on a VLAN.

## Examples

This example shows how to enable DHCP snooping on VLAN 10:

```
Switch(config)# ip dhcp snooping vlan 10
```

You can verify your settings by entering the **show ip dhcp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# ip dhcp snooping vlan information option format-type circuit-id string

Use the **ip dhcp snooping vlan information option format-type circuit-id string** interface configuration command to configure the option-82 circuit-ID suboption. Use the **no** form of this command to configure the default circuit-ID suboption.

**ip dhcp snooping vlan** *vlan* **information option format-type circuit-id string** *ASCII-string*

**no ip dhcp snooping vlan** *vlan* **information option format-type circuit-id string**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan* | Specify the VLAN ID. The range is 1 to 4094. |
| **string** *ASCII-string* | Specify a circuit ID, using from 3 to 63 ASCII characters (no spaces). |

## Defaults

The switch VLAN and the port identifier, in the format **vlan-mod-port**, is the default circuit ID.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SEG | This command was introduced. |

## Usage Guidelines

You must globally enable DHCP snooping by using the **ip dhcp snooping** global configuration command for any DHCP snooping configuration to take effect.

When the option-82 feature is enabled, the default circuit-ID suboption is the switch VLAN and the port identifier, in the format **vlan-mod-port**. This command allows you to configure a string of ASCII characters to be the circuit ID.

**Note** When configuring a large number of circuit IDs on a switch, consider the impact of lengthy character strings on the NVRAM or flash memory. If the circuit-ID configurations, combined with other data, exceed the capacity of the NVRAM or the flash memory, an error message appears.

## Examples

This example shows how to configure the option-82 circuit-ID suboption:

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
string customerABC-250-0-0
```

You can verify your settings by entering the **show ip dhcp snooping** user EXEC command.

**Note** The **show ip dhcp snooping** user EXEC command only displays the global command output, including a remote-ID configuration. It does not display any per-interface, per-VLAN string that you have configured for the circuit ID.

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping information option format remote-id** | Configures the option-82 remote-ID suboption. |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |

# ip igmp filter

Use the **ip igmp filter** interface configuration command to control whether or not all hosts on a Layer 2 interface can join one or more IP multicast groups by applying an Internet Group Management Protocol (IGMP) profile to the interface. Use the **no** form of this command to remove the specified profile from the interface.

**ip igmp filter** *profile number*

**no ip igmp filter**

## Syntax Description

| | |
|---|---|
| *profile number* | The IGMP profile number to be applied. The range is 1 to 4294967295. |

## Defaults

No IGMP filters are applied.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can apply IGMP filters only to Layer 2 physical interfaces; you cannot apply IGMP filters to ports that belong to an EtherChannel group.

An IGMP profile can be applied to one or more switch port interfaces, but one port can have only one profile applied to it.

## Examples

This example shows how to apply IGMP profile 22 to a port.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp filter 22
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

## Related Commands

| Command | Description |
|---|---|
| **ip igmp profile** | Configures the specified IGMP profile number. |
| **show ip dhcp snooping statistics** | Displays the characteristics of the specified IGMP profile. |
| **show running-config interface** *interface-id* | Displays the running configuration on the switch interface, including the IGMP profile (if any) that is applied to an interface. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |

# ip igmp max-groups

Use the **ip igmp max-groups** interface configuration command to set the maximum number of Internet Group Management Protocol (IGMP) groups that a Layer 2 interface can join or to configure the IGMP throttling action when the maximum number of entries is in the forwarding table. Use the **no** form of this command to set the maximum back to the default, which is to have no maximum limit, or to return to the default throttling action, which is to drop the report.

**ip igmp max-groups** {*number* | **action** {**deny** | **replace**}}

**no ip igmp max-groups** {*number* | **action**}

## Syntax Description

| | |
|---|---|
| *number* | The maximum number of IGMP groups that an interface can join. The range is 0 to 4294967294. The default is no limit. |
| **action deny** | When the maximum number of entries is in the IGMP snooping forwarding table, drop the next IGMP join report. This is the default action. |
| **action replace** | When the maximum number of entries is in the IGMP snooping forwarding table, replace the existing group with the new group for which the ICMP report was received. |

## Defaults

The default maximum number of groups is no limit.

After the switch learns the maximum number of IGMP group entries on an interface, the default throttling action is to drop the next IGMP report that the interface receives and to not add an entry for the IGMP group to the interface.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can use this command only on Layer 2 physical interfaces and on logical EtherChannel interfaces. You cannot set IGMP maximum groups for ports that belong to an EtherChannel group.

Follow these guidelines when configuring the IGMP throttling action:

- If you configure the throttling action as **deny** and set the maximum group limitation, the entries that were previously in the forwarding table are not removed but are aged out. After these entries are aged out, when the maximum number of entries is in the forwarding table, the switch drops the next IGMP report received on the interface.
- If you configure the throttling action as **replace** and set the maximum group limitation, the entries that were previously in the forwarding table are removed. When the maximum number of entries is in the forwarding table, the switch replaces a randomly-selected multicast entry with the received IGMP report.
- When the maximum group limitation is set to the default (no maximum), entering the **ip igmp max-groups** {**deny | replace**} command has no effect.

## Examples

This example shows how to limit to 25 the number of IGMP groups that a port can join.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# ip igmp max-groups 25
```

This example shows how to configure the switch to replace the existing group with the new group for which the IGMP report was received when the maximum number of entries is in the forwarding table:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# ip igmp max-groups action replace
```

You can verify your setting by using the **show running-config** privileged EXEC command and by specifying an interface.

## Related Commands

| Command | Description |
|---|---|
| **show running-config interface** *interface-id* | Displays the running configuration on the switch interface, including the maximum number of IGMP groups that an interface can join and the throttling action. For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > File Management Commands > Configuration File Management Commands**. |

# ip igmp profile

Use the **ip igmp profile** global configuration command to create an Internet Group Management Protocol (IGMP) profile and enter IGMP profile configuration mode. From this mode, you can specify the configuration of the IGMP profile to be used for filtering IGMP membership reports from a switchport. Use the **no** form of this command to delete the IGMP profile.

**ip igmp profile** *profile number*

**no ip igmp profile** *profile number*

## Syntax Description

| | |
|---|---|
| *profile number* | The IGMP profile number being configured. The range is 1 to 4294967295. |

## Defaults

No IGMP profiles are defined. When configured, the default action for matching an IGMP profile is to deny matching addresses.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2.(25)EX | This command was introduced. |

## Usage Guidelines

When you are in IGMP profile configuration mode, you can create the profile by using these commands:

- **deny**: specifies that matching addresses are denied; this is the default condition.
- **exit**: exits from igmp-profile configuration mode.
- **no**: negates a command or resets to its defaults.
- **permit**: specifies that matching addresses are permitted.
- **range**: specifies a range of IP addresses for the profile. This can be a single IP address or a range with a start and an end address.

  When entering a range, enter the low IP multicast address, a space, and the high IP multicast address.

You can apply an IGMP profile to one or more Layer 2 interfaces, but each interface can have only one profile applied to it.

## Examples

This example shows how to configure IGMP profile 40 that permits the specified range of IP multicast addresses.

```
Switch(config)# ip igmp profile 40
Switch(config-igmp-profile)# permit
Switch(config-igmp-profile)# range 233.1.1.1 233.255.255.255
```

You can verify your settings by using the **show ip igmp profile** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp filter** | Applies the IGMP profile to the specified interface. |
| **show ip dhcp snooping statistics** | Displays the characteristics of all IGMP profiles or the specified IGMP profile number. |

# ip igmp snooping

Use the **ip igmp snooping** global configuration command to globally enable Internet Group Management Protocol (IGMP) snooping on the switch or to enable it on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**ip igmp snooping** [**vlan** *vlan-id*]

**no ip igmp snooping** [**vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. |

## Defaults

IGMP snooping is globally enabled on the switch.

IGMP snooping is enabled on VLAN interfaces.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When IGMP snooping is enabled globally, it is enabled in all the existing VLAN interfaces. When IGMP snooping is disabled globally, it is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

## Examples

This example shows how to globally enable IGMP snooping:

```
Switch(config)# ip igmp snooping
```

This example shows how to enable IGMP snooping on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp snooping report-suppression** | Enables IGMP report suppression. |
| **show ip igmp snooping** | Displays the snooping configuration. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information. |
| **show ip igmp snooping mrouter** | Displays the IGMP snooping router ports. |
| **show ip igmp snooping querier detail** | Displays the configuration and operation information for the IGMP querier configured on a switch. |

# ip igmp snooping last-member-query-interval

Use the **ip igmp snooping last-member-query-interval** global configuration command to enable the Internet Group Management Protocol (IGMP) configurable-leave timer globally or on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**ip igmp snooping [vlan** *vlan-id*] **last-member-query-interval** *time*

**no ip igmp snooping [vlan** *vlan-id*] **last-member-query-interval**

## Syntax Descriptiont

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Enable IGMP snooping and the leave timer on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. |
| *time* | Interval time out in seconds. The range is 100 to 5000 milliseconds. |

## Defaults

The default timeout setting is 1000 milliseconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When IGMP snooping is globally enabled, IGMP snooping is enabled on all the existing VLAN interfaces. When IGMP snooping is globally disabled, IGMP snooping is disabled on all the existing VLAN interfaces.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Configuring the leave timer on a VLAN overrides the global setting.

The IGMP configurable leave time is only supported on devices running IGMP Version 2.

The configuration is saved in NVRAM.

## Examples

This example shows how to globally enable the IGMP leave timer for 2000 milliseconds:

```
Switch(config)# ip igmp snooping last-member-query-interval 2000
```

This example shows how to configure the IGMP leave timer for 3000 milliseconds on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 last-member-query-interval 3000
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp snooping** | Enables IGMP snooping on the switch or on a VLAN. |
| **ip igmp snooping vlan immediate-leave** | Enables IGMP Immediate-Leave processing. |
| **ip igmp snooping vlan mrouter** | Configures a Layer 2 port as a multicast router port. |
| **ip igmp snooping vlan static** | Configures a Layer 2 port as a member of a group. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration. |

# ip igmp snooping querier

Use the **ip igmp snooping querier** global configuration command to globally enable the Internet Group Management Protocol (IGMP) querier function in Layer 2 networks. Use the command with keywords to enable and configure the IGMP querier feature on a VLAN interface. Use the **no** form of this command to return to the default settings.

**ip igmp snooping querier** [**vlan** *vlan-id*] [**address** *ip-address* | **max-response-time** *response-time* | **query-interval** *interval-count* | **tcn query** [**count** *count* | **interval** *interval*] | **timer expiry** | **version** *version*]

**no ip igmp snooping querier** [**vlan** *vlan-id*] [**address | max-response-time | query-interval | tcn query** { **count** *count* | **interval** *interval*} | **timer expiry | version**]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Enable IGMP snooping and the IGMP querier function on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. |
| **address** *ip-address* | (Optional) Specify a source IP address. If you do not specify an IP address, the querier tries to use the global IP address configured for the IGMP querier. |
| **max-response-time** *response-time* | (Optional) Set the maximum time to wait for an IGMP querier report. The range is 1 to 25 seconds. |
| **query-interval** *interval-count* | (Optional) Set the interval between IGMP queriers. The range is 1 to 18000 seconds. |
| **tcn query [count** *count* **\| interval** *interval*] | (Optional) Set parameters related to Topology Change Notifications (TCNs). The keywords have these meanings:<br>• **count** *count*—Set the number of TCN queries to be executed during the TCN interval time. The range is 1 to 10.<br>• **interval** *interval*—Set the TCN query interval time. The range is 1 to 255. |
| **timer expiry** | (Optional) Set the length of time until the IGMP querier expires. The range is 60 to 300 seconds. |
| **version** *version* | (Optional) Select the IGMP version number that the querier feature uses. Select 1 or 2. |

## Defaults

The IGMP snooping querier feature is globally disabled on the switch.

When enabled, the IGMP snooping querier disables itself if it detects IGMP traffic from a multicast-enabled device.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to enable IGMP snooping to detect the IGMP version and IP address of a device that sends IGMP query messages, which is also called a *querier*.

By default, the IGMP snooping querier is configured to detect devices that use IGMP *Version 2* (IGMPv2) but does not detect clients that are using IGMP *Version 1* (IGMPv1). You can manually configure the **max-response-time** value when devices use IGMPv2. You cannot configure the **max-response-time** when devices use IGMPv1. (The value cannot be configured and is set to zero).

Non-RFC compliant devices running IGMPv1 might reject IGMP general query messages that have a non-zero value as the **max-response-time** value. If you want the devices to accept the IGMP general query messages, configure the IGMP snooping querier to run IGMPv1.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

## Examples

This example shows how to globally enable the IGMP snooping querier feature:

```
Switch(config)# ip igmp snooping querier
```

This example shows how to set the IGMP snooping querier maximum response time to 25 seconds:

```
Switch(config)# ip igmp snooping querier max-response-time 25
```

This example shows how to set the IGMP snooping querier interval time to 60 seconds:

```
Switch(config)# ip igmp snooping querier query-interval 60
```

This example shows how to set the IGMP snooping querier TCN query count to 25:

```
Switch(config)# ip igmp snooping querier tcn count 25
```

This example shows how to set the IGMP snooping querier timeout to 60 seconds:

```
Switch(config)# ip igmp snooping querier timeout expiry 60
```

This example shows how to set the IGMP snooping querier feature to version 2:

```
Switch(config)# ip igmp snooping querier version 2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping report-suppression** | Enables IGMP report suppression. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information. |
| **show ip igmp snooping mrouter** | Displays the IGMP snooping router ports. |

# ip igmp snooping report-suppression

Use the **ip igmp snooping report-suppression** global configuration command to enable Internet Group Management Protocol (IGMP) report suppression. Use the **no** form of this command to disable IGMP report suppression and to forward all IGMP reports to multicast routers.

**ip igmp snooping report-suppression**

**no ip igmp snooping report-suppression**

## Syntax Description

This command has no arguments or keywords.

## Defaults

IGMP report suppression is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

IGMP report suppression is supported only when the multicast query has IGMPv1 and IGMPv2 reports. This feature is not supported when the query includes IGMPv3 reports.

The switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices. When IGMP router suppression is enabled (the default), the switch sends the first IGMP report from all hosts for a group to all the multicast routers. The switch does not send the remaining IGMP reports for the group to the multicast routers. This feature prevents duplicate reports from being sent to the multicast devices.

If the multicast router query includes requests only for IGMPv1 and IGMPv2 reports, the switch forwards only the first IGMPv1 or IGMPv2 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for IGMPv3 reports, the switch forwards all IGMPv1, IGMPv2, and IGMPv3 reports for a group to the multicast devices.

If you disable IGMP report suppression by entering the **no ip igmp snooping report-suppression** command, all IGMP reports are forwarded to all the multicast routers.

## Examples

This example shows how to disable report suppression:

```
Switch(config)# no ip igmp snooping report-suppression
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| ip igmp snooping | Enables IGMP snooping on the switch or on a VLAN. |
| show ip igmp snooping | Displays the IGMP snooping configuration of the switch or the VLAN. |

# ip igmp snooping tcn

Use the **ip igmp snooping tcn** global configuration command to configure the Internet Group Management Protocol (IGMP) Topology Change Notification (TCN) behavior. Use the **no** form of this command to return to the default settings.

**ip igmp snooping tcn** {**flood query count** *count* | **query solicit**}

**no ip igmp snooping tcn** {**flood query count** | **query solicit**}

## Syntax Description

| | |
|---|---|
| **flood query count** *count* | Specify the number of IGMP general queries for which the multicast traffic is flooded. The range is 1 to 10. |
| **query solicit** | Send an IGMP leave message (global leave) to speed the process of recovering from the flood mode caused during a TCN event. |

## Defaults

The TCN flood query count is 2.

The TCN query solicitation is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can prevent the loss of the multicast traffic that might occur because of a topology change by using this command. If you set the TCN flood query count to 1 by using the ip **igmp snooping tcn flood query count** command, the flooding stops after receiving one general query. If you set the count to 7, the flooding of multicast traffic due to the TCN event lasts until seven general queries are received. Groups are relearned based on the general queries received during the TCN event.

## Examples

This example shows how to specify 7 as the number of IGMP general queries for which the multicast traffic is flooded:

```
Switch(config)# no ip igmp snooping tcn flood query count 7
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping | Enables IGMP snooping on the switch or on a VLAN. |
| ip igmp snooping tcn flood | Specifies flooding on an interface as the IGMP snooping spanning-tree TCN behavior. |
| show ip igmp snooping | Displays the IGMP snooping configuration of the switch or the VLAN. |

# ip igmp snooping tcn flood

Use the **ip igmp snooping tcn flood** interface configuration command to specify multicast flooding as the Internet Group Management Protocol (IGMP) snooping spanning-tree Topology Change Notification (TCN) behavior. Use the **no** form of this command to disable the multicast flooding.

**ip igmp snooping tcn flood**

**no ip igmp snooping tcn flood**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Multicast flooding is enabled on an interface during a spanning-tree TCN event.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When the switch receives a TCN, multicast traffic is flooded to all the ports until two general queries are received. If the switch has many ports with attached hosts that are subscribed to different multicast groups, this flooding behavior might not be desirable because the flooded traffic might exceed the capacity of the link and cause packet loss.

You can change the flooding query count by using the **ip igmp snooping tcn flood query count** *count* global configuration command.

## Examples

This example shows how to disable the multicast flooding on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no ip igmp snooping tcn flood
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping | Enables IGMP snooping on the switch or on a VLAN. |
| ip igmp snooping tcn | Configures the IGMP TCN behavior on the switch. |
| show ip igmp snooping | Displays the IGMP snooping configuration of the switch or the VLAN. |

# ip igmp snooping vlan immediate-leave

Use the **ip igmp snooping vlan** *vlan-id* **immediate-leave** global configuration command to enable Internet Group Management Protocol (IGMP) snooping immediate-leave processing on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**ip igmp snooping vlan** *vlan-id* **immediate-leave**

**no ip igmp snooping vlan** *vlan-id* **immediate-leave**

## Syntax Description

| | |
|---|---|
| *vlan-id* | Enable IGMP snooping and the Immediate-Leave feature on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. |

## Defaults

IGMP immediate-leave processing is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

You should only configure the Immediate Leave feature when there is a maximum of one receiver on every port in the VLAN. The configuration is saved in NVRAM.

The Immediate Leave feature is supported only with IGMP Version 2 hosts.

## Examples

This example shows how to enable IGMP immediate-leave processing on VLAN 1:

```
Switch(config)# ip igmp snooping vlan 1 immediate-leave
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping report-suppression** | Enables IGMP report suppression. |
| **show ip igmp snooping** | Displays the snooping configuration. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information. |
| **show ip igmp snooping mrouter** | Displays the IGMP snooping router ports. |
| **show ip igmp snooping querier detail** | Displays the configuration and operation information for the IGMP querier configured on a switch. |

# ip igmp snooping vlan mrouter

Use the **ip igmp snooping vlan** *vlan-id* **mrouter** global configuration command to add a multicast router port or to configure the multicast learning method. Use the **no** form of this command to return to the default settings.

**ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

**no ip igmp snooping vlan** *vlan-id* **mrouter** {**interface** *interface-id* | **learn pim-dvmrp**}

## Syntax Description

| | |
|---|---|
| *vlan-id* | Enable IGMP snooping, and add the port in the specified VLAN as the multicast router port. The range is 1 to 1001 and 1006 to 4094. |
| **interface** *interface-id* | Specify the next-hop interface to the multicast router. Valid interfaces are physical interfaces and port channels. The port-channel range is 1 to 48. |
| **learn pim-dvmrp** | Specify the multicast router learning method. The only learning method supported on the Cisco ME switch is **pim-dvmrp**, which sets the switch to learn multicast router ports by snooping on IGMP queries and Protocol-Independent Multicast-Distance Vector Multicast Routing Protocol (PIM-DVMRP) packets. |

## Defaults

By default, there are no multicast router ports.

The default learning method is **pim-dvmrp**—to snoop IGMP queries and PIM-DVMRP packets.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

## Examples

This example shows how to configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp snooping report-suppression** | Enables IGMP report suppression. |
| **show ip igmp snooping** | Displays the snooping configuration. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information. |
| **show ip igmp snooping mrouter** | Displays the IGMP snooping router ports. |
| **show ip igmp snooping querier detail** | Displays the configuration and operation information for the IGMP querier configured on a switch. |

# ip igmp snooping vlan static

Use the **ip igmp snooping vlan** *vlan-id* **static** global configuration command to enable Internet Group Management Protocol (IGMP) snooping and to statically add a Layer 2 port as a member of a multicast group. Use the **no** form of this command to remove ports specified as members of a static multicast group.

**ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-id*

**no ip igmp snooping vlan** *vlan-id* **static** *ip-address* **interface** *interface-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | Enable IGMP snooping on the specified VLAN. The range is 1 to 1001 and 1006 to 4094. |
| *ip-address* | Add a Layer 2 port as a member of a multicast group with the specified group IP address. |
| **interface** *interface-id* | Specify the interface of the member port. The keywords have these meanings:<br>• **fastethernet** *interface number*—a Fast Ethernet IEEE 802.3 interface.<br>• **gigabitethernet** *interface number*—a Gigabit Ethernet IEEE 802.3z interface.<br>• **port-channel** *interface number*—a channel interface. The range is 0 to 48. |

## Defaults

By default, there are no ports statically configures as members of a multicast group.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

The configuration is saved in NVRAM.

## Examples

This example shows how to statically configure a port as a multicast router port:

```
Switch(config)# ip igmp snooping vlan 1 mrouter interface gigabitethernet0/2
```

You can verify your settings by entering the **show ip igmp snooping** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp snooping report-suppression** | Enables IGMP report suppression. |
| **show ip igmp snooping** | Displays the snooping configuration. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information. |
| **show ip igmp snooping mrouter** | Displays the IGMP snooping router ports. |
| **show ip igmp snooping querier detail** | Displays the configuration and operation information for the IGMP querier configured on a switch. |

# ip ssh

Use the **ip ssh** global configuration command to configure the switch to run Secure Shell (SSH) Version 1 or SSH Version 2. Use the **no** form of this command to return to the default setting.

**ip ssh version** [**1** | **2**]

**no ip ssh version** [**1** | **2**]

This command is available only when your switch is running the cryptographic (encrypted) software image.

## Syntax Description

| | |
|---|---|
| **1** | (Optional) Configure the switch to run SSH Version 1 (SSHv1). |
| **2** | (Optional) Configure the switch to run SSH Version 2 (SSHv1). |

## Defaults

The default version is the latest SSH version supported by the SSH client.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not enter this command or if you do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.

The switch supports an SSHv1 or an SSHv2 server. It also supports an SSHv1 client. For more information about the SSH server and the SSH client, see the software configuration guide for this release.

A Rivest, Shamir, and Adelman (RSA) key pair generated by an SSHv1 server can be used by an SSHv2 server and the reverse.

## Examples

This example shows how to configure the switch to run SSH Version 2:

```
Switch(config)# ip ssh version 2
```

You can verify your settings by entering the **show ip ssh** or **show ssh** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show ip ssh** | Displays if the SSH server is enabled and displays the version and configuration information for the SSH server. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands**. |
| **show ssh** | Displays the status of the SSH server. For syntax information, select **Cisco IOS Release 12.2 Configuration Guides and Command References > Cisco IOS Security Command Reference, Release 12.2 > Other Security Features > Secure Shell Commands**. |

# lacp port-priority

Use the **lacp port-priority** interface configuration command to configure the port priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lacp port-priority** *priority*

**no lacp port-priority**

**Note** LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *priority* | Port priority for LACP. The range is 1 to 65535. |

## Defaults

The default is 32768.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **lacp port-priority** interface configuration command determines which ports are bundled and which ports are put in hot-standby mode when there are more than eight ports in an LACP channel group. This command takes effect only on EtherChannel ports that are already configured for LACP. If the interface is a user network interface (UNI), you must use the **port-type nni** or **port-type eni** interface configuration command to change the interface to an NNI or ENI before configuring **lacp port-priority**.

In priority comparisons, numerically *lower* values have *higher* priority. The switch uses the priority to decide which ports should be put in standby mode when there is a hardware limitation that prevents all compatible ports from being active. If two or more ports have the same LACP port priority (for example, they are configured with the default setting of 65535), an internal value for the port number determines the priority.

**Note** The LACP port priorities are only effective if the ports are on the switch that controls the LACP link. See the **lacp system-priority** global configuration command for information about determining which switch controls the link.

Use the **show lacp internal** privileged EXEC command to display LACP port priorities and internal port number values.

For information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

## Examples

This example shows how to configure the LACP port priority on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# lacp port-priority 1000
```

You can verify your settings by entering the **show lacp** [*channel-group-number*] **internal** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns an Ethernet port to an EtherChannel group. |
| **lacp system-priority** | Configures the LACP system priority. |
| **show lacp** [*channel-group-number*] **internal** | Displays internal information for all channel groups or for the specified channel group. |

# lacp system-priority

Use the **lacp system-priority** global configuration command to configure the system priority for the Link Aggregation Control Protocol (LACP). Use the **no** form of this command to return to the default setting.

**lacp system-priority** *priority*

**no lacp system-priority**

**Note** LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *priority* | System priority for LACP. The range is 1 to 65535. |

## Defaults

The default is 32768.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **lacp system-priority** command determines which switch in an LACP link controls port priorities. Although this is a global configuration command, the priority only takes effect on EtherChannels that have physical ports that are already configured for LACP.

An LACP channel group can have up to 16 Ethernet ports of the same type. Up to eight ports can be active, and up to eight ports can be in standby mode. When there are more than eight ports in an LACP channel group, the switch on the controlling end of the link uses port priorities to determine which ports are bundled into the channel and which ports are put in hot-standby mode. Port priorities on the other switch (the noncontrolling end of the link) are ignored.

In priority comparisons, numerically lower values have higher priority. Therefore, the switch with the numerically lower system value (higher priority value) for LACP system priority becomes the controlling switch. If both switches have the same LACP system priority (for example, they are both configured with the default setting of 32768), the LACP system ID (the switch MAC address) determines which switch is in control.

The **lacp system-priority** command applies to all LACP EtherChannels on the switch.

Use the **show etherchannel summary** privileged EXEC command to see which ports are in the hot-standby mode (denoted with an H port-state flag).

For more information about configuring LACP on physical ports, see the “Configuring EtherChannels” chapter in the software configuration guide for this release.

## Examples

This example shows how to set the LACP system priority:

```
Switch(config)# lacp system-priority 20000
```

You can verify your settings by entering the **show lacp sys-id** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns an Ethernet port to an EtherChannel group. |
| **lacp port-priority** | Configures the LACP port priority. |
| **show lacp sys-id** | Displays the system identifier that is being used by LACP. |

# logging event

Use the **logging event** interface configuration command to enable notification of interface link status changes. Use the **no** form of this command to disable notification.

**logging event** {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

**no logging event** {**bundle-status** | **link-status** | **spanning-tree** | **status** | **trunk status**}

## Syntax Description

| | |
|---|---|
| **bundle-status** | Enable notification of BUNDLE and UNBUNDLE messages. |
| **link-status** | Enable notification of interface data link status changes. |
| **spanning-tree** | Enable notification of spanning-tree events. |
| **status** | Enable notification of spanning-tree state change messages. |
| **trunk-status** | Enable notification of trunk-status messages. |

## Defaults

Event logging is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SEG | This command was introduced. |

## Examples

This example shows how to enable spanning-tree logging:

```
Switch(config-if)# logging event spanning-tree
```

# logging file

Use the **logging file** global configuration command to set logging file parameters. Use the **no** form of this command to return to the default setting.

**logging file** *filesystem*:*filename* [*max-file-size* [*min-file-size*]] [*severity-level-number* | *type*]

**no logging file** *filesystem*:*filename* [*severity-level-number* | *type*]

## Syntax Description

| | |
|---|---|
| filesystem:*filename* | Alias for a flash file system. Contains the path and name of the file that contains the log messages.<br>The syntax for the local flash file system:<br>**flash:** |
| *max-file-size* | (Optional) Specify the maximum logging file size. The range is 4096 to 2147483647. |
| *min-file-size* | (Optional) Specify the minimum logging file size. The range is 1024 to 2147483647. |
| *severity-level-number* | (Optional) Specify the logging severity level. The range is 0 to 7. See the *type* option for the meaning of each level. |
| *type* | (Optional) Specify the logging type. These keywords are valid:<br>• **emergencies**—System is unusable (severity 0).<br>• **alerts**—Immediate action needed (severity 1).<br>• **critical**—Critical conditions (severity 2).<br>• **errors**—Error conditions (severity 3).<br>• **warnings**—Warning conditions (severity 4).<br>• **notifications**—Normal but significant messages (severity 5).<br>• **information**—Information messages (severity 6).<br>• **debugging**—Debugging messages (severity 7). |

## Defaults

The minimum file size is 2048 bytes; the maximum file size is 4096 bytes.

The default severity level is 7 (**debugging** messages and numerically lower levels).

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The log file is stored in ASCII text format in an internal buffer on the switch. You can access logged system messages by using the switch command-line interface (CLI) or by saving them to a properly configured syslog server. If the switch fails, the log is lost unless you had previously saved it to flash memory by using the **logging file flash:***filename* global configuration command.

After saving the log to flash memory by using the **logging file flash:***filename* global configuration command, you can use the **more flash:***filename* privileged EXEC command to display its contents.

The command rejects the minimum file size if it is greater than the maximum file size minus 1024; the minimum file size then becomes the maximum file size minus 1024.

Specifying a *level* causes messages at that level and numerically lower levels to be displayed.

## Examples

This example shows how to save informational log messages to a file in flash memory:

```
Switch(config)# logging file flash:logfile informational
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# mac access-group

Use the **mac access-group** interface configuration command to apply a MAC access control list (ACL) to a Layer 2 interface. Use the **no** form of this command to remove all MAC ACLs or the specified MAC ACL from the interface. You create the MAC ACL by using the **mac access-list extended** global configuration command.

**mac access-group** {*name*} **in**

**no mac access-group** {*name*}

## Syntax Description

| | |
|---|---|
| *name* | Specify a named MAC access list. |
| **in** | Specify that the ACL is applied in the ingress direction. Outbound ACLs are not supported on Layer 2 interfaces. |

## Defaults

No MAC ACL is applied to the interface.

## Command Modes

Interface configuration (Layer 2 interfaces only)

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can apply MAC ACLs only to ingress Layer 2 interfaces.

On Layer 2 interfaces, you can filter IP traffic by using IP access lists and non-IP traffic by using MAC access lists. You can filter both IP and non-IP traffic on the same Layer 2 interface by applying both an IP ACL and a MAC ACL to the interface. You can apply no more than one IP access list and one MAC access list to the same Layer 2 interface.

If a MAC ACL is already configured on a Layer 2 interface and you apply a new MAC ACL to the interface, the new ACL replaces the previously configured one.

If you apply an ACL to a Layer 2 interface on a switch, and the switch has a VLAN map applied to a VLAN that the interface is a member of, the ACL applied to the Layer 2 interface takes precedence.

When an inbound packet is received on an interface with a MAC ACL applied, the switch checks the match conditions in the ACL. If the conditions are matched, the switch forwards or drops the packet, according to the ACL.

If the specified ACL does not exist, the switch forwards all packets.

**Note** For more information about configuring MAC extended ACLs, see the "Configuring Network Security with ACLs" chapter in the software configuration guide for this release.

## Examples

This example shows how to apply a MAC extended ACL named *macacl2* to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mac access-group macacl2 in
```

You can verify your settings by entering the **show mac access-group** privileged EXEC command. You can see configured ACLs on the switch by entering the **show access-lists** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show access-lists** | Displays the ACLs configured on the switch. |
| **show mac access-group** | Displays the MAC ACLs configured on the switch. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# mac access-list extended

Use the **mac access-list extended** global configuration command to create an access list based on MAC addresses for non-IP traffic. Using this command puts you in the extended MAC access-list configuration mode. Use the **no** form of this command to return to the default setting.

**mac access-list extended** *name*

**no mac access-list extended** *name*

## Syntax Description

| | |
|---|---|
| *name* | Assign a name to the MAC extended access list. |

## Defaults

By default, there are no MAC access lists created.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

MAC named extended lists are used with VLAN maps and class maps.

You can apply named MAC extended ACLs to VLAN maps or to Layer 2 interfaces.

Entering the **mac access-list extended** command enables the MAC access-list configuration mode. These configuration commands are available:

- **default**: sets a command to its default.
- **deny**: specifies packets to reject. For more information, see the deny (MAC access-list configuration) MAC access-list configuration command.
- **exit**: exits from MAC access-list configuration mode.
- **no**: negates a command or sets its defaults.
- **permit**: specifies packets to forward. For more information, see the permit (MAC access-list configuration) command.

**Note** For more information about MAC extended access lists, see the software configuration guide for this release.

## Examples

This example shows how to create a MAC named extended access list named *mac1* and to enter extended MAC access-list configuration mode:

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)#
```

This example shows how to delete MAC named extended access list *mac1*:

```
Switch(config)# no mac access-list extended mac1
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **deny (MAC access-list configuration)** | Configures the MAC ACL (in extended MAC-access list configuration mode). |
| **permit (MAC access-list configuration)** | |
| **show access-lists** | Displays the access lists configured on the switch. |
| **vlan access-map** | Defines a VLAN map and enters access-map configuration mode where you can specify a MAC ACL to match and the action to be taken. |

# mac address-table aging-time

Use the **mac address-table aging-time** global configuration command to set the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. Use the **no** form of this command to return to the default setting. The aging time applies to all VLANs or a specified VLAN.

**mac address-table aging-time** {**0** | *10-1000000*} [**vlan** *vlan-id*]

**no mac address-table aging-time** {**0** | *10-1000000*} [**vlan** *vlan-id*]

## Syntax DescriptionI

| | |
|---|---|
| **0** | This value disables aging. Static address entries are never aged or removed from the table. |
| *10-1000000* | Aging time in seconds. The range is 10 to 1000000 seconds. |
| **vlan** *vlan-id* | (Optional) Specify the VLAN ID to which to apply the aging time. The range is 1 to 4094. |

## Defaults

The default is 300 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If hosts do not send continuously, increase the aging time to record the dynamic entries for a longer time. Increasing the time can reduce the possibility of flooding when the hosts send again.

If you do not specify a specific VLAN, this command sets the aging time for all VLANs.

## Examples

This example shows how to set the aging time to 200 seconds for all VLANs:

```
Switch(config)# mac address-table aging-time 200
```

You can verify your setting by entering the **show mac address-table aging-time** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table aging-time** | Displays the MAC address table aging time for all VLANs or the specified VLAN. |

# mac address-table notification

Use the **mac address-table notification** global configuration command to enable the MAC address notification feature on the switch. Use the **no** form of this command to return to the default setting.

**mac address-table notification** [**history-size** *value*] | [**interval** *value*]

**no mac address-table notification** [**history-size** | **interval**]

## Syntax Description

| | |
|---|---|
| **history-size** *value* | (Optional) Configure the maximum number of entries in the MAC notification history table. The range is 1 to 500 entries. |
| **interval** *value* | (Optional) Set the notification trap interval. The switch sends the notification traps when this amount of time has elapsed. The range is 0 to 2147483647 seconds. |

## Defaults

By default, the MAC address notification feature is disabled.

The default trap interval value is 1 second.

The default number of entries in the history table is 1.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Whenever a new MAC address is added or an old address is deleted from the forwarding tables, the MAC address notification feature sends Simple Network Management Protocol (SNMP) traps to a network management system (NMS). MAC notifications are generated only for dynamic and secure MAC addresses. Events are not generated for self addresses, multicast addresses, or other static addresses.

When you configure the **history-size** option, the existing MAC address history table is deleted, and a new table is created.

You enable the MAC address notification feature by using the **mac address-table notification** command. You must also enable MAC address notification traps on an interface by using the **snmp trap mac-notification** interface configuration command and configure the switch to send MAC address traps to the NMS by using the **snmp-server enable traps mac-notification** global configuration command.

## Examples

This example shows how to enable the MAC address-table notification feature, set the interval time to 60 seconds, and set the history-size to 100 entries:

```
Switch(config)# mac address-table notification
Switch(config)# mac address-table notification interval 60
Switch(config)# mac address-table notification history-size 100
```

You can verify your settings by entering the **show mac address-table notification** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **clear mac address-table notification** | Clears the MAC address notification global counters. |
| **show mac address-table notification** | Displays the MAC address notification settings on all interfaces or on the specified interface. |
| **snmp-server enable traps** | Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended. |
| **snmp trap mac-notification** | Enables the SNMP MAC notification trap on a specific interface. |

# mac address-table static

Use the **mac address-table static** global configuration command to add static addresses to the MAC address table. Use the **no** form of this command to remove static entries from the table.

**mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id*

**no mac address-table static** *mac-addr* **vlan** *vlan-id* [**interface** *interface-id*]

## Syntax Description

| | |
|---|---|
| *mac-addr* | Destination MAC address (unicast or multicast) to add to the address table. Packets with this destination address received in the specified VLAN are forwarded to the specified interface. |
| **vlan** *vlan-id* | Specify the VLAN for which the packet with the specified MAC address is received. The range is 1 to 4094. |
| **interface** *interface-id* | Interface to which the received packet is forwarded. Valid interfaces include physical ports and port channels. |

## Defaults

No static addresses are configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to add the static address c2f3.220a.12f4 to the MAC address table. When a packet is received in VLAN 4 with this MAC address as its destination, the packet is forwarded to the specified interface:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 interface
gigabitethernet0/1
```

You can verify your setting by entering the **show mac address-table** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table static** | Displays static MAC address table entries only. |

# mac address-table static drop

Use the **mac address-table static drop** global configuration command to enable unicast MAC address filtering and to configure the switch to drop traffic with a specific source or destination MAC address. Use the **no** form of this command to return to the default setting.

**mac address-table static** *mac-addr* **vlan** *vlan-id* **drop**

**no mac address-table static** *mac-addr* **vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *mac-addr* | Unicast source or destination MAC address. Packets with this MAC address are dropped. |
| **vlan** *vlan-id* | Specify the VLAN for which the packet with the specified MAC address is received. Valid VLAN IDs are 1 to 4094. |

## Defaults

Unicast MAC address filtering is disabled. The switch does not drop traffic for specific source or destination MAC addresses.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Follow these guidelines when using this feature:

- Multicast MAC addresses, broadcast MAC addresses, and router MAC addresses are not supported. Packets that are forwarded to the CPU are also not supported.
- If you add a unicast MAC address as a static address and configure unicast MAC address filtering, the switch either adds the MAC address as a static address or drops packets with that MAC address, depending on which command was entered last. The second command that you entered overrides the first command.

  For example, if you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** command, the switch drops packets with the specified MAC address as a source or destination.

  If you enter the **mac address-table static** *mac-addr* **vlan** *vlan-id* **drop** global configuration command followed by the **mac address-table static** *mac-addr* **vlan** *vlan-id* **interface** *interface-id* command, the switch adds the MAC address as a static address.

## Examples

This example shows how to enable unicast MAC address filtering and to configure the switch to drop packets that have a source or destination address of c2f3.220a.12f4. When a packet is received in VLAN 4 with this MAC address as its source or destination, the packet is dropped:

```
Switch(config)# mac address-table static c2f3.220a.12f4 vlan 4 drop
```

This example shows how to disable unicast MAC address filtering:

```
Switch(config)# no mac address-table static c2f3.220a.12f4 vlan 4
```

You can verify your setting by entering the **show mac address-table static** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table static** | Displays only static MAC address table entries. |

# macro apply

Use the **macro apply** interface configuration command to apply a macro to an interface or to apply and trace a macro configuration on an interface.

**macro** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

## Syntax Description

| | |
|---|---|
| **apply** | Apply a macro to the specified interface. |
| **trace** | Use the **trace** keyword to apply a macro to an interface and to debug the macro. |
| *macro-name* | Specify the name of the macro. |
| **parameter** *value* | (Optional) Specify unique parameter values that are specific to the interface. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. |

## Defaults

This command has no default setting.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can use the **macro trace** *macro-name* interface configuration command to apply and show the macros running on an interface or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the interface.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the interface.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro apply** *macro-name* **?** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to an interface, the macro name is automatically added to the interface. You can display the applied commands and macro names by using the **show running-configuration interface** *interface-id* user EXEC command.

A macro applied to an interface range behaves the same way as a macro applied to a single interface. When you use an interface range, the macro is applied sequentially to each interface within the range. If a macro command fails on one interface, it is still applied to the remaining interfaces.

You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command.

## Examples

After you have created a macro by using the **macro name** global configuration command, you can apply it to an interface. This example shows how to apply a user-created macro called **duplex** to an interface:

```
Switch(config-if)# macro apply duplex
```

To debug a macro, use the **macro trace** interface configuration command to find any syntax or configuration errors in the macro as it is applied to an interface. This example shows how troubleshoot the user-created macro called **duplex** on an interface:

```
Switch(config-if)# macro trace duplex
Applying command...'duplex auto'
%Error Unknown error.
Applying command...'speed nonegotiate'
```

## Related Commands

| Command | Description |
|---|---|
| **macro description** | Adds a description about the macros that are applied to an interface. |
| **macro global** | Applies a macro on a switch or applies and traces a macro on a switch. |
| **macro global description** | Adds a description about the macros that are applied to the switch. |
| **macro name** | Creates a macro. |
| **show parser macro** | Displays the macro definition for all macros or for the specified macro. |

# macro description

Use the **macro description** interface configuration command to enter a description about which macros are applied to an interface. Use the **no** form of this command to remove the description.

**macro description** *text*

**no macro description** *text*

## Syntax Description

| | |
|---|---|
| **description** *text* | Enter a description about the macros that are applied to the specified interface. |

## Defaults

This command has no default setting.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with an interface. When multiple macros are applied on a single interface, the description text will be from the last applied macro.

This example shows how to add a description to an interface:

```
Switch(config-if)# macro description duplex settings
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **macro apply** | Applies a macro on an interface or applies and traces a macro on an interface. |
| **macro global** | Applies a macro on a switch or applies and traces a macro on a switch |
| **macro global description** | Adds a description about the macros that are applied to the switch. |
| **macro name** | Creates a macro. |
| **show parser macro** | Displays the macro definition for all macros or for the specified macro. |

# macro global

Use the **macro global** global configuration command to apply a macro to a switch or to apply and trace a macro configuration on a switch.

**macro global** {**apply** | **trace**} *macro-name* [**parameter** {*value*}] [**parameter** {*value*}] [**parameter** {*value*}]

## Syntax Description

| | |
|---|---|
| **apply** | Apply a macro to the switch. |
| **trace** | Apply a macro to a switch and to debug the macro. |
| *macro-name* | Specify the name of the macro. |
| **parameter** *value* | (Optional) Specify unique parameter values that are specific to the switch. You can enter up to three keyword-value pairs. Parameter keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. |

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can use the **macro trace** *macro-name* global configuration command to apply and to show the macros running on a switch or to debug the macro to find any syntax or configuration errors.

If a command fails because of a syntax error or a configuration error when you apply a macro, the macro continues to apply the remaining commands to the switch.

When creating a macro that requires the assignment of unique values, use the **parameter** *value* keywords to designate values specific to the switch.

Keyword matching is case sensitive. All matching occurrences of the keyword are replaced with the corresponding value. Any full match of a keyword, even if it is part of a larger string, is considered a match and is replaced by the corresponding value.

Some macros might contain keywords that require a parameter value. You can use the **macro global apply** *macro-name* **?** command to display a list of any required values in the macro. If you apply a macro without entering the keyword values, the commands are invalid and are not applied.

When you apply a macro to a switch, the macro name is automatically added to the switch. You can display the applied commands and macro names by using the **show running-configuration** user EXEC command.

You can delete a global macro-applied configuration on a switch only by entering the **no** version of each command contained in the macro.

## Examples

After you have created a new macro by using the **macro name** global configuration command, you can apply it to a switch. This example shows how see the **snmp** macro and how to apply the macro and set the hostname to test-server and set the IP precedence value to 7:

```
Switch# show parser macro name snmp
Macro name : snmp
Macro type : customizable

#enable port security, linkup, and linkdown traps
snmp-server enable traps port-security
snmp-server enable traps linkup
snmp-server enable traps linkdown
#set snmp-server host
snmp-server host ADDRESS
#set SNMP trap notifications precedence
snmp-server ip precedence VALUE

------------------------------------------------
Switch(config)# macro global apply snmp ADDRESS test-server VALUE 7
```

To debug a macro, use the **macro global trace** global configuration command to find any syntax or configuration errors in the macro when it is applied to a switch. In this example, the **ADDRESS** parameter value was not entered, causing the `snmp-server host` command to fail while the remainder of the macro is applied to the switch:

```
Switch(config)# macro global trace snmp VALUE 7
Applying command...'snmp-server enable traps port-security'
Applying command...'snmp-server enable traps linkup'
Applying command...'snmp-server enable traps linkdown'
Applying command...'snmp-server host'
%Error Unknown error.
Applying command...'snmp-server ip precedence 7'
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply** | Applies a macro on an interface or applies and traces a macro on an interface. |
| **macro description** | Adds a description about the macros that are applied to an interface. |
| **macro global description** | Adds a description about the macros that are applied to the switch. |
| **macro name** | Creates a macro. |
| **show parser macro** | Displays the macro definition for all macros or for the specified macro. |

# macro global description

Use the **macro global description** global configuration command to enter a description about the macros that are applied to the switch. Use the **no** form of this command to remove the description.

**macro global description** *text*

**no macro global description** *text*

## Syntax Description

| | |
|---|---|
| **description** *text* | Enter a description about the macros that are applied to the switch. |

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **description** keyword to associate comment text, or the macro name, with a switch. When multiple macros are applied on a switch, the description text will be from the last applied macro.

This example shows how to add a description to a switch:

```
Switch(config)# macro global description udld aggressive mode enabled
```

You can verify your settings by entering the **show parser macro description** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **macro apply** | Applies a macro on an interface or applies and traces a macro on an interface. |
| **macro description** | Adds a description about the macros that are applied to an interface. |
| **macro global** | Applies a macro on a switch or applies and traces a macro on a switch. |
| **macro name** | Creates a macro. |
| **show parser macro** | Displays the macro definition for all macros or for the specified macro. |

# macro name

Use the **macro name** global configuration command to create a configuration macro. Use the **no** form of this command to delete the macro definition.

**macro name** *macro-name*

**no macro name** *macro-name*

## Syntax Description

| | |
|---|---|
| *macro-name* | Name of the macro. |

## Defaults

This command has no default setting.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A macro can contain up to 3000 characters. Enter one macro command per line. Use the @ character to end the macro. Use the # character at the beginning of a line to enter comment text within the macro.

You can define mandatory keywords within a macro by using a help string to specify the keywords. Enter **# macro keywords** *word* to define the keywords that are available for use with the macro. You can enter up to three help string keywords separated by a space. If you enter more than three macro keywords, only the first three are shown.

Macro names are case sensitive. For example, the commands **macro name Sample-Macro** and **macro name sample-macro** will result in two separate macros.

When creating a macro, do not use the **exit** or **end** commands or change the command mode by using **interface** *interface-id*. This could cause commands that follow **exit**, **end**, or **interface** *interface-id* to execute in a different command mode.

The **no** form of this command only deletes the macro definition. It does not affect the configuration of those interfaces on which the macro is already applied. You can delete a macro-applied configuration on an interface by entering the **default interface** *interface-id* interface configuration command. Alternatively, you can create an *anti-macro* for an existing macro that contains the **no** form of all the corresponding commands in the original macro. Then apply the anti-macro to the interface.

You can modify a macro by creating a new macro with the same name as the existing macro. The newly created macro overwrites the existing macro but does not affect the configuration of those interfaces on which the original macro was applied.

## Examples

This example shows how to create a macro that defines the duplex mode and speed:

```
Switch(config)# macro name duplex
Enter macro commands one per line. End with the character '@'.
duplex full
speed auto
@
```

This example shows how create a macro with **# macro keywords**:

```
Switch(config)# macro name test
switchport access vlan $VLANID
switchport port-security maximum $MAX
#macro keywords $VLANID $MAX
@
```

This example shows how to display the mandatory keyword values before you apply the macro to an interface:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# macro apply test ?
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID ?
  WORD  Value of first keyword to replace

Switch(config-if)# macro apply test $VLANID 2
  WORD  keyword to replace with a value e.g  $VLANID,$MAX
  <cr>

Switch(config-if)# macro apply test $VLANID 2 $MAX ?
  WORD  Value of second keyword to replace
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply** | Applies a macro on an interface or applies and traces a macro on an interface. |
| **macro description** | Adds a description about the macros that are applied to an interface. |
| **macro global** | Applies a macro on a switch or applies and traces a macro on a switch |
| **macro global description** | Adds a description about the macros that are applied to the switch. |
| **show parser macro** | Displays the macro definition for all macros or for the specified macro. |

# match (access-map configuration)

Use the **match** access-map configuration command to set the VLAN map to match packets against one or more access lists. Use the **no** form of this command to remove the match parameters.

**match** {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

**no match** {**ip address** {*name* | *number*} [*name* | *number*] [*name* | *number*]...} | {**mac address** {*name*} [*name*] [*name*]...}

## Syntax Description

| | |
|---|---|
| **ip address** | Set the access map to match packets against an IP address access list. |
| **mac address** | Set the access map to match packets against a MAC address access list. |
| *name* | Name of the access list to match packets against. |
| *number* | Number of the access list to match packets against. This option is not valid for MAC access lists. |

## Defaults

The default action is to have no match parameters applied to a VLAN map.

## Command Modes

Access-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You enter access-map configuration mode by using the **vlan access-map** global configuration command.

You must enter one access list name or number; others are optional. You can match packets against one or more access lists. Matching any of the lists counts as a match of the entry.

In access-map configuration mode, use the **match** command to define the match conditions for a VLAN map applied to a VLAN. Use the **action** command to set the action that occurs when the packet matches the conditions.

Packets are matched only against access lists of the same protocol type; IP packets are matched against IP access lists, and all other packets are matched against MAC access lists.

Both IP and MAC addresses can be specified for the same map entry.

## Examples

This example shows how to define and apply a VLAN access map *vmap4* to VLANs 5 and 6 that will cause the interface to drop an IP packet if the packet matches the conditions defined in access list *al2*.

```
Switch(config)# vlan access-map vmap4
Switch(config-access-map)# match ip address al2
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan filter vmap4 vlan-list 5-6
```

You can verify your settings by entering the **show vlan access-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Configures a standard numbered ACL. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**. |
| **action** | Specifies the action to be taken if the packet matches an entry in an access control list (ACL). |
| **ip access list** | Creates a named access list. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands**. |
| **mac access-list extended** | Creates a named MAC address access list. |
| **show vlan access-map** | Displays the VLAN access maps created on the switch. |
| **vlan access-map** | Creates a VLAN access map. |

# match access-group

Use the **match access-group** class-map configuration command to configure the match criteria for a class map on the basis of the specified access control list (ACL). Use the **no** form of this command to remove the ACL match criteria.

**match access-group** *acl-index-or-name*

**no match access-group** *acl-index-or-name*

## Syntax Description

| | |
|---|---|
| *acl-index-or-name* | Number or name of an IP standard or extended access control list (ACL) or MAC ACL. For an IP standard ACL, the ACL index range is 1 to 99 and 1300 to 1999. For an IP extended ACL, the ACL index range is 100 to 199 and 2000 to 2699. |

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **match access-group** command specifies a numbered or named ACL to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match access-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match access-group** classification only on input policy maps.

## Examples

This example shows how to create a class map called in*class*, which uses the access control list *acl1* as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **show class-map** | Displays quality of service (QoS) class maps. |

# match cos

Use the **match cos** class-map configuration command to match a packet based on a Layer 2 class of service (CoS) marking. Use the **no** form of this command to remove the CoS match criteria.

**match cos** *cos-list* |

**no match cos** *cos-list*

## Syntax Description

| | |
|---|---|
| *cos-list* | List of up to four CoS values to match against incoming packets. Separate each value with a space. The range is 0 to 7. |

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **match cos** command specifies a CoS value to use as the match criteria to determine if packets belong to the class specified by the class map.

Before using the **match cos** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

Matching of CoS values is supported only on ports carrying Layer 2 VLAN-tagged traffic. That is, you can use the **cos** classification only on IEEE 802.1Q trunk ports.

You can use **match cos** classification in input and output policy maps.

## Examples

This example shows how to create a class map called in*class*, which matches all the incoming traffic with CoS values of 1 and 4:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match cos 1 4
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **show class-map** | Displays quality of service (QoS) class maps. |

# match ip dscp

Use the **match ip dscp** class-map configuration command to identify a specific IPv4 Differentiated Service Code Point (DSCP) value as match criteria for a class. Use the **no** form of this command to remove the match criteria.

**match ip dscp** *dscp-list*

**no match ip dscp** *dscp-list*

## Syntax Description

| | |
|---|---|
| *ip-dscp-list* | List of up to eight IPv4 DSCP values to match against incoming packets. Separate each value with a space. The range is 0 to 63. You can also enter a mnemonic name for a commonly used value.<br>See the "Configuring QoS" chapter in the software configuration guide for this release for information about other options for specifying DSCP values. |

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **match ip dscp** command specifies a DSCP value to use as the match criteria to determine if packets belong to the class specified by the class map.

This command is used by the class map to identify a specific DSCP value marking on a packet. In this context, DSCP values are used as markings only and have no mathematical significance. For example, the DSCP value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip dscp** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to eight DSCP values in one match statement. For example, if you wanted the DCSP values of 0, 1, 2, 3, 4, 5, 6, or 7, enter the **match ip dscp 0 1 2 3 4 5 6 7** command. The packet must match only one (not all) of the specified IPv4 DSCP values to belong to the class.

You can use **match ip dscp** classification in input and output policy maps.

## Examples

This example shows how to create a class map called in*class*, which matches all the incoming traffic with DSCP values of 10, 11, and 12:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **show class-map** | Displays quality of service (QoS) class maps. |

# match ip precedence

Use the **match ip precedence** class-map configuration command to identify IPv4 precedence values as match criteria for a class. Use the **no** form of this command to remove the match criteria.

**match ip precedence** *ip-precedence-list*

**no match ip precedence** *ip-precedence-list*

## Syntax Description

| | |
|---|---|
| **ip precedence** *ip-precedence-list* | List of up to four IPv4 precedence values to match against incoming packets. Separate each value with a space. The range is 0 to 7. |

## Defaults

No match criteria are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **match ip precedence** command specifies an IPv4 precedence value to use as the match criteria to determine if packets belong to the class specified by the class map.

The precedence values are used as marking only. In this context, the IP precedence values have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

Before using the **match ip precedence** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can enter up to four IPv4 precedence values in one match statement. For example, if you wanted the IP precedence values of 0, 1, 2, or 7, enter the **match ip precedence 0 1 2 7** command. The packet must match only one (not all) of the specified IP precedence values to belong to the class.

You can use **match ip precedence** classification in input and output policy maps.

## Examples

This example shows how to create a class map called *class*, which matches all the incoming traffic with IP-precedence values of 5, 6, and 7:

```
Switch(config)# class-map match-any in-class
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **show class-map** | Displays quality of service (QoS) class maps. |

# match qos-group

Use the **match qos-group** class-map configuration command to identify a specific quality of service (QoS) group value as a match criterion for a class. Use the **no** form of this command to remove the match criterion.

**match qos-group** *value*

**no match qos-group** *value*

## Syntax Description

| | |
|---|---|
| **qos-group** *value* | A quality of service group value. The range is from 0 to 99. |

## Defaults

No match criterion are defined.

## Command Modes

Class-map configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The QoS group range was extended to from 0 to 99. |

## Usage Guidelines

The **match qos-group** command specifies a QoS group value to use as the match criterion to determine if packets belong to the class specified by the class map.

The QoS-group values are used as marking only and have no mathematical significance. For example, the precedence value of 2 is not greater than 1, but merely indicates that a packet marked with a value of 2 is different than one marked with a value of 1. You define the treatment of these marked packets by setting QoS policies in policy-map class configuration mode.

The QoS-group value is local to the switch, meaning that the QoS-group value marked on a packet does not leave the switch when the packet leaves the switch. If you require a marking that remains with the packet, use IP Differentiated Service Code Point (DSCP) values, IP precedence values, or another method of packet marking.

Before using the **match qos-group** command, you must enter the **class-map** global configuration command to specify the name of the class whose match criteria you want to establish.

You can use the **match qos-group** classification only on output policy maps.

There can be no more than 100 QoS groups on the switch (0 to 99).

## Examples

This example shows how to classify traffic by using QoS group 13 as the match criterion:

```
Switch(config)# class-map match-any inclass
Switch(config-cmap)# match qos-group 13
Switch(config-cmap)# exit
```

You can verify your settings by entering the **show class-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| class-map | Creates a class map to be used for matching packets to the class whose name you specify. |
| show class-map | Displays QoS class maps. |

# mdix auto

Use the **mdix auto** interface configuration command to enable the automatic medium-dependent interface crossover (auto-MDIX) feature on the interface. When auto-MDIX is enabled, the interface automatically detects the required cable connection type (straight-through or crossover) and configures the connection appropriately. Use the **no** form of this command to disable auto-MDIX.

**mdix auto**

**no mdix auto**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Auto-MDIX is enabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you enable auto-MDIX on an interface, you must also set the speed and duplex on the interface to **auto** so that the feature operates correctly. If the port is a user network interface (UNI) or enhanced network interfaces (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **mdix auto** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

When auto-MDIX (along with autonegotiation of speed and duplex) is enabled on one or both of connected interfaces, link up occurs, even if the required cable type (straight-through or crossover) is not present.

Auto-MDIX is supported on all 10/100-Mbps interfaces and on 10/100/1000BASE-T/BASE-TX small form-factor pluggable (SFP)-module interfaces. It is not supported on 1000BASE-SX or -LX SFP module interfaces.

## Examples

This example shows how to enable auto-MDIX on a port:

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto
Switch(config-if)# duplex auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

You can verify the operational state of auto-MDIX on the interface by entering the **show controllers ethernet-controller** *interface-id* **phy** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show controllers ethernet-controller** *interface-id* **phy** | Displays general information about internal registers of an interface, including the operational state of auto-MDIX. |

# monitor session

Use the **monitor session** global configuration command to start a new Switched Port Analyzer (SPAN) session or Remote SPAN (RSPAN) source or destination session, to enable incoming traffic on the destination port for a network security device (such as a Cisco IDS Sensor Appliance), to add or delete interfaces or VLANs to or from an existing SPAN or RSPAN session, and to limit (filter) SPAN source traffic to specific VLANs. Use the **no** form of this command to remove the SPAN or RSPAN session or to remove source or destination interfaces or filters from the SPAN or RSPAN session. For destination interfaces, the **encapsulation dot1q** or **encapsulation replicate** keywords are ignored with the **no** form of the command.

**monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}] | {**remote vlan** *vlan-id*}

**monitor session** *session_number* **filter vlan** *vlan-id* [, | -]

**monitor session** *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]}| {**remote vlan** *vlan-id*}

**no monitor session** {*session_number* | **all** | **local** | **remote**}

**no monitor session** *session_number* **destination** {**interface** *interface-id* [, | -] [**encapsulation** {**dot1q** | **replicate**}] [**ingress** {[**dot1q** | **untagged**] **vlan** *vlan-id*}] | {**remote vlan** *vlan-id*}

**no monitor session** *session_number* **filter vlan** *vlan-id* [, | -]

**no monitor session** *session_number* **source** {**interface** *interface-id* [, | -] [**both** | **rx** | **tx**]} | {**vlan** *vlan-id* [, | -] [**both** | **rx** | **tx**]} | {**remote vlan** *vlan-id*}

## Syntax Description

| | |
|---|---|
| *session_number* | Specify the session number identified with the SPAN or RSPAN session. The range is 1 to 66. |
| **interface** *interface-id* | Specify the destination or source interface for a SPAN or RSPAN session. Valid interfaces are physical ports (including type and port number). For **source interface**, **port channel** is also a valid interface type, and the valid range is 1 to 48. |
| **destination** | Specify the SPAN or RSPAN destination. A destination must be a physical port. |
| **encapsulation replicate** | (Optional) Specify the encapsulation method. If not selected, the default is to send packets in native form (untagged).<br>• **dot1q**—Specify IEEE 802.1Q encapsulation.<br>• **replicate—**Specify that the destination interface replicates the source interface encapsulation method.<br>**Note** Entering these keywords is valid only for local SPAN. For RSPAN, the RSPAN VLAN ID overwrites the original VLAN ID; therefore packets are always sent untagged. |
| **ingress** | (Optional) Enable ingress traffic forwarding. |
| **dot1q vlan** *vlan-id* | Specify ingress forwarding using IEEE 802.1Q encapsulation with the specified VLAN as the default VLAN for ingress traffic. |

| | |
|---|---|
| **untagged vlan** *vlan-id* | Specify ingress forwarding using untagged encapsulation with the specified VLAN as the default VLAN for ingress traffic |
| **vlan** *vlan-id* | When used with only the **ingress** keyword, set default VLAN for ingress traffic. |
| **remote vlan** *vlan-id* | Specify the remote VLAN for an RSPAN source or destination session. The range is 2 to 1001 and 1006 to 4094.<br>**Note** The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs). |
| **,** | (Optional) Specify a series of interfaces or VLANs, or separate a range of interfaces or VLANs from a previous range. Enter a space before and after the comma. |
| **-** | (Optional) Specify a range of interfaces or VLANs. Enter a space before and after the hyphen. |
| **filter vlan** *vlan-id* | Specify a list of VLANs as filters on trunk source ports to limit SPAN source traffic to specific VLANs. The *vlan-id* range is 1 to 4094. |
| **source** | Specify the SPAN or RSPAN source. A source can be a physical port, a port channel, or a VLAN. |
| **both, rx, tx** | (Optional) Specify the traffic direction to monitor. If you do not specify a traffic direction, the source interface sends both transmitted and received traffic. |
| **source vlan** *vlan-id* | Specify the SPAN source interface as a VLAN ID. The range is 1 to 4094. |
| **all**, **local**, **remote** | Specify **all**, **local**, or **remote** with the **no monitor session** command to clear all SPAN and RSPAN, all local SPAN, or all RSPAN sessions. |

## Defaults

No monitor sessions are configured.

On a source interface, the default is to monitor both received and transmitted traffic.

On a trunk interface used as a source port, all VLANs are monitored.

If **encapsulation dot1q** or **encapsulation replicate** is not specified on a local SPAN destination port, packets are sent in native form with no encapsulation tag.

Ingress forwarding is disabled on destination ports.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Traffic that enters or leaves source ports or source VLANs can be monitored by using SPAN or RSPAN. Traffic routed to source ports or source VLANs cannot be monitored.

You can set a combined maximum of two local SPAN sessions and RSPAN source sessions. You can have a total of 66 SPAN and RSPAN sessions on a switch.

You can have a maximum of 64 destination ports on a switch.

Each session can include multiple ingress or egress source ports or VLANs, but you cannot combine source ports and source VLANs in a single session. Each session can include multiple destination ports.

When you use VLAN-based SPAN (VSPAN) to analyze network traffic in a VLAN or set of VLANs, all active ports in the source VLANs become source ports for the SPAN or RSPAN session. Trunk ports are included as source ports for VSPAN, and only packets with the monitored VLAN ID are sent to the destination port.

You can monitor traffic on a single port or VLAN or on a series or range of ports or VLANs. You select a series or range of interfaces or VLANs by using the [**,** | **-**] options.

If you specify a series of VLANs or interfaces, you must enter a space before and after the comma. If you specify a range of VLANs or interfaces, you must enter a space before and after the hyphen (**-**).

EtherChannel ports cannot be configured as SPAN or RSPAN destination ports. A physical port that is a member of an EtherChannel group can be used as a destination port, but it cannot participate in the EtherChannel group while it is as a SPAN destination.

A private-VLAN port cannot be configured as a SPAN destination port.

You can monitor individual ports while they participate in an EtherChannel, or you can monitor the entire EtherChannel bundle by specifying the **port-channel** number as the RSPAN source interface.

A port used as a destination port cannot be a SPAN or RSPAN source, nor can a port be a destination port for more than one session at a time.

You can enable IEEE 802.1x on a port that is a SPAN or RSPAN destination port; however, IEEE 802.1x is disabled until the port is removed as a SPAN destination. (If IEEE 802.1x is not available on the port, the switch returns an error message.) You can enable IEEE 802.1x on a SPAN or RSPAN source port.

VLAN filtering refers to analyzing network traffic on a selected set of VLANs on trunk source ports. By default, all VLANs are monitored on trunk source ports. You can use the **monitor session** *session_number* **filter vlan** *vlan-id* command to limit SPAN traffic on trunk source ports to only the specified VLANs.

VLAN monitoring and VLAN filtering are mutually exclusive. If a VLAN is a source, VLAN filtering cannot be enabled. If VLAN filtering is configured, a VLAN cannot become a source.

If ingress traffic forwarding is enabled for a network security device, the destination port forwards traffic at Layer 2.

Destination ports can be configured to act in these ways:

- When you enter **monitor session** *session_number* **destination interface** *interface-id* with no other keywords, egress encapsulation is untagged, and ingress forwarding is not enabled.
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate** with no other keywords, egress encapsulation replicates the source interface encapsulation; ingress forwarding is not enabled. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)

- When you enter **monitor session** *session_number* **destination interface** *interface-id* **encapsulation replicate ingress**, egress encapsulation replicates the source interface encapsulation; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**. (This applies to local SPAN only; RSPAN does not support encapsulation replication.)
- When you enter **monitor session** *session_number* **destination interface** *interface-id* **ingress**, egress encapsulation is untagged; ingress encapsulation depends on the keywords that follow—**dot1q** or **untagged**.

## Examples

This example shows how to create a local SPAN session 1 to monitor both sent and received traffic on source port 1 to destination port 2:

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1 both
Switch(config)# monitor session 1 destination interface gigabitethernet0/2
```

This example shows how to delete a destination port from an existing local SPAN session:

```
Switch(config)# no monitor session 2 destination gigabitethernet0/2
```

This example shows how to limit SPAN traffic in an existing session only to specific VLANs:

```
Switch(config)# monitor session 1 filter vlan 100 - 110
```

This example shows how to configure RSPAN source session 1 to monitor multiple source interfaces and to configure the destination RSPAN VLAN 900.

```
Switch(config)# monitor session 1 source interface gigabitethernet0/1
Switch(config)# monitor session 1 source interface port-channel 2 tx
Switch(config)# monitor session 1 destination remote vlan 900
Switch(config)# end
```

This example shows how to configure an RSPAN destination session 10 in the switch receiving the monitored traffic.

```
Switch(config)# monitor session 10 source remote vlan 900
Switch(config)# monitor session 10 destination interface gigabitethernet0/2
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that supports IEEE 802.1Q encapsulation. Egress traffic replicates the source; ingress traffic uses IEEE 802.1Q encapsulation.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 encapsulation
replicate ingress dot1q vlan 5
```

This example shows how to configure the destination port for ingress traffic on VLAN 5 by using a security device that does not support encapsulation. Egress traffic and ingress traffic are untagged.

```
Switch(config)# monitor session 2 destination interface gigabitethernet0/2 ingress
untagged vlan 5
```

You can verify your settings by entering the **show monitor** privileged EXEC command. You can display SPAN and RSPAN configuration on the switch by entering the **show running-config** privileged EXEC command. SPAN information appears near the end of the output.

## Related Commands

| Command | Description |
|---|---|
| **remote-span** | Configures an RSPAN VLAN in vlan configuration mode. |
| **show monitor** | Displays SPAN and RSPAN session information. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# mvr (global configuration)

Use the **mvr** global configuration command without keywords to enable the multicast VLAN registration (MVR) feature on the switch. Use the command with keywords to set the MVR mode for a switch, configure the MVR IP multicast address, set the maximum time to wait for a query reply before removing a port from group membership, and to specify the MVR multicast VLAN. Use the **no** form of this command to return to the default settings.

**mvr** [**group** *ip-address* [*count*] | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

**no mvr** [**group** *ip-address* | **mode** [**compatible** | **dynamic**] | **querytime** *value* | **vlan** *vlan-id*]

## Syntax Description

| | |
|---|---|
| **group** *ip-address* | Statically configure an MVR group IP multicast address on the switch.<br>Use the **no** form of this command to remove a statically configured IP multicast address or contiguous addresses or, when no IP address is entered, to remove all statically configured MVR IP multicast addresses. |
| *count* | (Optional) Configure multiple contiguous MVR group addresses. The range is 1 to 256; the default is 1. |
| **mode** | (Optional) Specify the MVR mode of operation.<br>The default is compatible mode. |
| **compatible** | Set MVR mode to provide compatibility with Catalyst 2900 XL and Catalyst 3500 XL switches. This mode does not allow dynamic membership joins on source ports. |
| **dynamic** | Set MVR mode to allow dynamic MVR membership on source ports. |
| **querytime** *value* | (Optional) Set the maximum time to wait for IGMP report memberships on a receiver port. This time applies only to receiver-port leave processing. When an IGMP query is sent from a receiver port, the switch waits for the default or configured MVR querytime for an IGMP group membership report before removing the port from multicast group membership.<br>The value is the response time in units of tenths of a second. The range is 1 to 100; the default is 5 tenths or one-half second.<br>Use the **no** form of the command to return to the default setting. |
| **vlan** *vlan-id* | (Optional) Specify the VLAN on which MVR multicast data is expected to be received. This is also the VLAN to which all the source ports belong. The range is 1 to 4094; the default is VLAN 1. |

## Defaults

MVR is disabled by default.

The default MVR mode is compatible mode.

No IP multicast addresses are configured on the switch by default.

The default group ip address count is 0.

The default query response time is 5 tenths of or one-half second.

The default multicast VLAN for MVR is VLAN 1.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

A maximum of 256 MVR multicast groups can be configured on a switch.

Use the **mvr group** command to statically set up all the IP multicast addresses that will take part in MVR. Any multicast data sent to a configured multicast address is sent to all the source ports on the switch and to all receiver ports that have registered to receive data on that IP multicast address.

MVR supports aliased IP multicast addresses on the switch. However, if the switch is interoperating with Catalyst 3550 or Catalyst 3500 XL switches, you should not configure IP addresses that alias between themselves or with the reserved IP multicast addresses (in the range 224.0.0.xxx).

The **mvr querytime** command applies only to receiver ports.

If the switch MVR is interoperating with Catalyst 2900 XL or Catalyst 3500 XL switches, set the multicast mode to compatible.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

MVR can coexist with IGMP snooping on a switch.

**Examples**

This example shows how to enable MVR:

```
Switch(config)# mvr
```

Use the **show mvr** privileged EXEC command to display the current setting for maximum multicast groups.

This example shows how to configure 228.1.23.4 as an IP multicast address:

```
Switch(config)# mvr group 228.1.23.4
```

This example shows how to configure ten contiguous IP multicast groups with multicast addresses from 228.1.23.1 to 228.1.23.10:

```
Switch(config)# mvr group 228.1.23.1 10
```

Use the **show mvr members** privileged EXEC command to display the IP multicast group addresses configured on the switch.

This example shows how to set the maximum query response time as one second (10 tenths):

```
Switch(config)# mvr querytime 10
```

This example shows how to set VLAN 2 as the multicast VLAN:

```
Switch(config)# mvr vlan 2
```

You can verify your settings by entering the **show mvr** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **mvr (interface configuration)** | Configures MVR ports. |
| **show mvr** | Displays MVR global parameters or port parameters. |
| **show mvr interface** | Displays the configured MVR interfaces with their type, mode, VLAN, status and Immediate Leave configuration, and can also displays all MVR groups of which the interface is a member. |
| **show mvr members** | Displays all ports that are members of an MVR multicast group; if the group has no members, its status is shown as Inactive. |

# mvr (interface configuration)

Use the **mvr** interface configuration command to configure a Layer 2 port as a multicast VLAN registration (MVR) receiver or source port, to set the Immediate Leave feature, and to statically assign a port to an IP multicast VLAN and IP address. Use the **no** form of this command to return to the default settings.

**mvr** {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}}

**no mvr** {**immediate** | **type** {**receiver** | **source**} | **vlan** *vlan-id* {[**group** *ip-address*] [**receiver vlan** *vlan-id*]}}

## Syntax Description

| | |
|---|---|
| **immediate** | (Optional) Enable the Immediate Leave feature of MVR on a port. Use the **no mvr immediate** command to disable the feature. |
| **type** | (Optional) Configure the port as an MVR receiver port or a source port.<br>The default port type is neither an MVR source nor a receiver port. The **no mvr type** command resets the port as neither a source or a receiver port. |
| **receiver** | Configure the port as a subscriber port that can only receive multicast data. Receiver ports cannot belong to the multicast VLAN. |
| **source** | Configure the port as an uplink port that can send and receive multicast data for the configured multicast groups. All source ports on a switch belong to a single multicast VLAN.<br>**Note** When you are configuring a trunk port as an MVR receiver port, we recommend that the source port is configured as a network node interface (NNI) and the MVR trunk receiver port is configured as a user node interface (UNI) or an enhanced network interface (ENI). |
| **vlan** *vlan-id* | Specify the mvr vlan for the system. |
| **group** *ip-address* | (Optional) Statically configure the specified MVR IP multicast group address for the specified multicast VLAN ID. This is the IP address of the multicast group that the port or VLAN is joining. |
| **receiver** vlan vlan-id | (Optional) Specify a receiver VLAN. |

## Defaults

A port is configured as neither a receiver nor a source.

The Immediate Leave feature is disabled on all ports.

No receiver port is a member of any configured multicast group.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SE | The **receiver** and *vlan-id* keywords were added. These are required to configure a trunk port as an MVR receiver port. |

## Usage Guidelines

Configure a port as a source port if that port should be able to both send and receive multicast data bound for the configured multicast groups. Multicast data is received on all ports configured as source ports.

Receiver ports on a switch can be in different VLANs, but should not belong to the multicast VLAN.

A port that is not taking part in MVR should not be configured as an MVR receiver port or a source port. A non-MVR port is a normal switch port, able to send and receive multicast data with normal switch behavior.

When Immediate Leave is enabled, a receiver port leaves a multicast group more quickly. Without Immediate Leave, when the switch receives an IGMP leave message from a group on a receiver port, it sends out an IGMP MAC-based query on that port and waits for IGMP group membership reports. If no reports are received in a configured time period, the receiver port is removed from multicast group membership. With Immediate Leave, an IGMP MAC-based query is not sent from the receiver port on which the IGMP leave was received. As soon as the leave message is received, the receiver port is removed from multicast group membership, which speeds up leave latency.

The Immediate Leave feature should be enabled only on receiver ports to which a single receiver device is connected.

The **mvr vlan group** command statically configures ports to receive multicast traffic sent to the IP multicast address. A port statically configured as a member of group remains a member of the group until statically removed. In compatible mode, this command applies only to receiver ports; in dynamic mode, it can also apply to source ports. Receiver ports can also dynamically join multicast groups by using IGMP join messages.

When operating in compatible mode, MVR does not support IGMP dynamic joins on MVR source ports.

An MVR port cannot be a private-VLAN port.

## Examples

This example shows how to configure a port as an MVR receiver port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr type receiver
```

Use the **show mvr interface** privileged EXEC command to display configured receiver ports and source ports.

This example shows how to enable Immediate Leave on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# mvr immediate
```

This example shows how to add a port on VLAN 1 as a static member of IP multicast group 228.1.23.4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan1 group 230.1.23.4
```

This example shows how to add a port 2 on VLAN 100 as a static member of IP multicast group 228.1.23.4. In this example, the receive port is an access port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# mvr vlan 100 group 228.1.23.4
```

This example shows how to add on port 5 the receiver VLAN 201 with an MVR VLAN of 100.

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 receiver vlan 201
```

This example shows how to add on port 5 the receiver VLAN 201 as a static member of the IP multicast group 239.1.1.1, with an MVR VLAN of 100:

```
Switch(config)# interface fastethernet0/5
Switch(config-if)# mvr vlan 100 group 239.1.1.1 receiver vlan 201
```

You can verify your settings by entering the **show mvr members** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **mvr (global configuration)** | Enables and configures multicast VLAN registration on the switch. |
| **show mvr** | Displays MVR global parameters or port parameters. |
| **show mvr interface** | Displays the configured MVR interfaces or displays the multicast groups to which a receiver port belongs. Also displays all MVR groups of which the interface is a member. |
| **show mvr members** | Displays all receiver ports that are members of an MVR multicast group. |

# pagp learn-method

Use the **pagp learn-method** interface configuration command to learn the source address of incoming packets received from an EtherChannel port. Use the **no** form of this command to return to the default setting.

**pagp learn-method** {**aggregation-port** | **physical-port**}

**no pagp learn-method**

**Note** PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| **aggregation-port** | Specify address learning on the logical port-channel. The switch sends packets to the source using any of the ports in the EtherChannel. This setting is the default. With aggregate-port learning, it is not important on which physical port the packet arrives. |
| **physical-port** | Specify address learning on the physical port within the EtherChannel. The switch sends packets to the source using the same port in the EtherChannel from which it learned the source address. The other end of the channel uses the same port in the channel for a particular destination MAC or IP address. |

## Defaults

The default is aggregation-port (logical port channel).

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the interface is a user network interface (UNI), you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring **pagp learn-method**. Learn must be configured to the same method at both ends of the link.

**Note** The Cisco ME switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

**Note** When the link partner to the Cisco ME switch is a physical learner, we recommend that you configure the switch as a physical-port learner. Use the **pagp learn-method physical-port** interface configuration command, and set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Only use the **pagp learn-method** interface configuration command in this situation.

## Examples

This example shows how to set the learning method to learn the address on the physical port within the EtherChannel:

```
Switch(config-if)# pagp learn-method physical-port
```

This example shows how to set the learning method to learn the address on the port-channel within the EtherChannel:

```
Switch(config-if)# pagp learn-method aggregation-port
```

You can verify your settings by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **pagp port-priority** | Selects a port over which all traffic through the EtherChannel is sent. |
| **show pagp** | Displays PAgP channel-group information. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# pagp port-priority

Use the **pagp port-priority** interface configuration command to select a port over which all Port Aggregation Protocol (PAgP) traffic through the EtherChannel is sent. If all unused ports in the EtherChannel are in hot-standby mode, they can be placed into operation if the currently selected port and link fails. Use the **no** form of this command to return to the default setting.

**pagp port-priority** *priority*

**no pagp port-priority**

**Note** PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *priority* | A priority number ranging from 0 to 255. |

## Defaults

The default is 128.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the interface is a user network interface (UNI), you must enter the **port-type nni** or **port-type eni** interface configuration command before configuring **pagp port-priority**.

The physical port with the highest operational priority and that has membership in the same EtherChannel is the one selected for PAgP transmission.

**Note** The Cisco ME switch supports address learning only on aggregate ports even though the **physical-port** keyword is provided in the command-line interface (CLI). The **pagp learn-method** and the **pagp port-priority** interface configuration commands have no effect on the switch hardware, but they are required for PAgP interoperability with devices that only support address learning by physical ports.

When the link partner to the Cisco ME **s**witch is a physical learner, we recommend that you configure the switch as a physical-port learner by using the **pagp learn-method physical-port** interface configuration command and to set the load-distribution method based on the source MAC address by using the **port-channel load-balance src-mac** global configuration command. Use the **pagp learn-method** interface configuration command only in this situation.

## Examples

This example shows how to set the port priority to 200:

```
Switch(config-if)# pagp port-priority 200
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show pagp** *channel-group-number* **internal** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **pagp learn-method** | Provides the ability to learn the source address of incoming packets. |
| **show pagp** | Displays PAgP channel-group information. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# permit (MAC access-list configuration)

Use the **permit** MAC access-list configuration command to allow non-IP traffic to be forwarded if the conditions are matched. Use the **no** form of this command to remove a permit condition from the extended MAC access list.

{**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** | **vines-ip** | **xns-idp**]

**no** {**permit** | **deny**} {**any** | **host** *src-MAC-addr* | *src-MAC-addr mask*} {**any** | **host** *dst-MAC-addr* | *dst-MAC-addr mask*} [*type mask* | **cos** *cos* | **aarp** | **amber** | **dec-spanning** | **decnet-iv** | **diagnostic** | **dsm** | **etype-6000** | **etype-8042** | **lat** | **lavc-sca** | **lsap** *lsap mask* | **mop-console** | **mop-dump** | **msdos** | **mumps** | **netbios** | **vines-echo** |**vines-ip** | **xns-idp**]

**Note** Though visible in the command-line help strings, **appletalk** is not supported as a matching condition.

## Syntax Description

| | |
|---|---|
| **any** | Keyword to specify to deny any source or destination MAC address. |
| **host** *src-MAC-addr* \| *src-MAC-addr mask* | Define a host MAC address and optional subnet mask. If the source address for a packet matches the defined address, non-IP traffic from that address is denied. |
| **host** *dst-MAC-addr* \| *dst-MAC-addr mask* | Define a destination MAC address and optional subnet mask. If the destination address for a packet matches the defined address, non-IP traffic to that address is denied. |
| *type mask* | (Optional) Use the Ethertype number of a packet with Ethernet II or SNAP encapsulation to identify the protocol of the packet.<br>• *type* is 0 to 65535, specified in hexadecimal.<br>• *mask* is a mask of *don't care* bits applied to the Ethertype before testing for a match. |
| **aarp** | (Optional) Select Ethertype AppleTalk Address Resolution Protocol that maps a data-link address to a network address. |
| **amber** | (Optional) Select EtherType DEC-Amber. |
| **cos** *cos* | (Optional) Select an arbitrary class of service (CoS) number from 0 to 7 to set priority. Filtering on CoS can be performed only in hardware. A warning message appears if the **cos** option is configured. |
| **dec-spanning** | (Optional) Select EtherType Digital Equipment Corporation (DEC) spanning tree. |
| **decnet-iv** | (Optional) Select EtherType DECnet Phase IV protocol. |
| **diagnostic** | (Optional) Select EtherType DEC-Diagnostic. |
| **dsm** | (Optional) Select EtherType DEC-DSM. |
| **etype-6000** | (Optional) Select EtherType 0x6000. |
| **etype-8042** | (Optional) Select EtherType 0x8042. |
| **lat** | (Optional) Select EtherType DEC-LAT. |
| **lavc-sca** | (Optional) Select EtherType DEC-LAVC-SCA. |

| | |
|---|---|
| **lsap** *lsap-number mask* | (Optional) Use the LSAP number (0 to 65535) of a packet with 802.2 encapsulation to identify the protocol of the packet.<br><br>The *mask* is a mask of *don't care* bits applied to the LSAP number before testing for a match. |
| **mop-console** | (Optional) Select EtherType DEC-MOP Remote Console. |
| **mop-dump** | (Optional) Select EtherType DEC-MOP Dump. |
| **msdos** | (Optional) Select EtherType DEC-MSDOS. |
| **mumps** | (Optional) Select EtherType DEC-MUMPS. |
| **netbios** | (Optional) Select EtherType DEC- Network Basic Input/Output System (NETBIOS). |
| **vines-echo** | (Optional) Select EtherType Virtual Integrated Network Service (VINES) Echo from Banyan Systems. |
| **vines-ip** | (Optional) Select EtherType VINES IP. |
| **xns-idp** | (Optional) Select EtherType Xerox Network Systems (XNS) protocol suite. |

To filter IPX traffic, you use the *type mask* or **lsap** *lsap mask* keywords, depending on the type of IPX encapsulation being used. Filter criteria for IPX encapsulation types as specified in Novell terminology and Cisco IOS terminology are listed in Table 2-3.

***Table 2-3 IPX Filtering Criteria***

| **IPX Encapsulation Type** | | |
|---|---|---|
| **Cisco IOS Name** | **Novell Name** | **Filter Criterion** |
| arpa | Ethernet II | Ethertype 0x8137 |
| snap | Ethernet-snap | Ethertype 0x8137 |
| sap | Ethernet 802.2 | LSAP 0xE0E0 |
| novell-ether | Ethernet 802.3 | LSAP 0xFFFF |

## Defaults

This command has no defaults. However, the default action for a MAC-named ACL is to deny.

## Command Modes

MAC access-list configuration

## Command History

| **Release** | **Modification** |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You enter MAC access-list configuration mode by using the **mac access-list extended** global configuration command.

If you use the **host** keyword, you cannot enter an address mask; if you do not use the **any** or **host** keywords, you must enter an address mask.

After an access control entry (ACE) is added to an access control list, an implied **deny**-**any**-**any** condition exists at the end of the list. That is, if there are no matches, the packets are denied. However, before the first ACE is added, the list permits all packets.

**Note** For more information about MAC-named extended access lists, see the software configuration guide for this release.

## Examples

This example shows how to define the MAC-named extended access list to allow NETBIOS traffic from any source to MAC address 00c0.00a0.03fa. Traffic matching this list is allowed.

```
Switch(config-ext-macl)# permit any host 00c0.00a0.03fa netbios
```

This example shows how to remove the permit condition from the MAC-named extended access list:

```
Switch(config-ext-macl)# no permit any 00c0.00a0.03fa 0000.0000.0000 netbios
```

This example permits all packets with Ethertype 0x4321:

```
Switch(config-ext-macl)# permit any any 0x4321 0
```

You can verify your settings by entering the **show access-lists** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **deny (MAC access-list configuration)** | Denies non-IP traffic to be forwarded if conditions are matched. |
| **mac access-list extended** | Creates an access list based on MAC addresses for non-IP traffic. |
| **show access-lists** | Displays access control lists configured on a switch. |

# police

Use the **police** policy-map class configuration command to define an individual policer for classified traffic and to enter policy-map class police configuration mode. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. In policy-map class police configuration mode, you can specify multiple actions for a packet. Use the **no** form of this command to remove an existing policer.

**police** {*rate-bps* | **cir** *cir-bps*} [*burst-bytes* | **bc** [*burst-value*]] [**conform-action** [**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

**no police** {*rate-bps* | **cir** *cir-bps*} [*burst-bytes* | **bc** [*burst-value*]] [**conform-action** [**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

**Note** When **police** is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported, and the *rate-bps* range is smaller. Only the default conform-action of **transmit** and the default exceed-action of **drop** are supported.

## Syntax Description

| | |
|---|---|
| *rate-bps* | Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000.<br>**Note** The range for **police** with the **priority** command for output service policies is 64000 to 1000000000. |
| **cir** | Committed information rate (CIR) used for policing traffic. |
| *cir-bps* | CIR rate in bps. The range is 8000 to 1000000000 bps.<br>**Note** The range for **police** with the **priority** command for output service policies is 64000 to 1000000000. |
| *burst-bytes* | (Optional) Specify the normal burst size in bytes. The range is 8000 to 1000000. |
| **bc** [*burst- value*] | (Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes. If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications. |

| | |
|---|---|
| **conform-action** | (Optional) Action to be taken for packets that conform to the CIR. |
| **set-cos-transmit** *new-cos-value* | Set a new class of service (CoS) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new CoS value is 0 to 7. |
| **set-dscp-transmit** *new-dscp-value* | Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new DCSP value is 0 to 63. |
| **set-prec-transmit** *new-precedence-value* | Set a new IP precedence value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new IP precedence value is 0 to 7. |
| **set-qos-transmit** *qos-group-value* | Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new QoS value is 0 to 99. |
| **cos** | (Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **dscp** | (Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **precedence** | (Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **table** *table-map name* | (Optional) Used in conjunction with the preceding *from-type* keyword. Specify the table map to be used for the enhanced packet marking. The *to-type* of the action is marked based on the *from-type* parameter of the action using this table map. |
| **transmit** | (Optional) Send the packet unmodified. |
| **exceed action** | (Optional) Action to be taken for packets that do not conform to the CIR. |
| **drop** | Drop the packet. |

## Defaults

No policers are defined. Conform burst (**bc**) is automatically configured to 250 ms at the configured CIR.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Increased support for configuring conform and exceed actions. See “Usage Guidelines.” |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking and configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking

provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.

The switch supports a maximum of 229 policer instances on the switch (228 user-configurable policers and 1 policer reserved for internal use). You can configure up to 46 policers on a port.

Policing is only supported in input policies or in output policies that were configured with the **priority** policy-map class configuration command to reduce bandwidth in the priority queue.

**Note** When used with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line interface help is 8000 to 1000000000. You cannot attach an output service policy with an out-of-range rate.

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

To configure multiple conform-actions or multiple exceed-actions, enter policy-map class police configuration mode, and use the **conform-action** and **exceed-action** policy-map class police configuration commands.

When you define the policer and enter a carriage return, you enter policy-map class police configuration mode, which allows you to configure multiple policing actions. In this mode, these configuration commands are available:

- **conform-action**: the action to be taken on packets that conform to the CIR. The default action is to **transmit** the packet. For more information, see the **conform-action** policy-map class police command.
- **exceed-action**: the action to be taken on packets that do not conform to the CIR. The default action is to **drop** the packet. For more information, see the **exceed-action** policy-map class police command.
- **exit**: exits from QoS policy-map class police configuration mode. If you do not want to set multiple actions, you can enter **exit** without entering any other policy-map class police commands.
- **no**: negate or set the default values of a command.

## Examples

This example shows how to configure a policer with a 1-Mbps average rate with a burst size of 20 KB. The policer sets a new DSCP precedence value if the packets conform to the rate and drops the packet if traffic exceeds the rate.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class inclass1
Switch(config-pmap-c)# police cir 1000000 20000 conform-action set-dscp-transmit 46
exceed-action drop
Switch(config-pmap-c)# exit
```

This example shows how to configure a policer with default actions.

```
Switch(config)# policy-map policy2
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police 1000000 20000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **conform-action** | Define multiple actions for a policy-map class for packets that meet the CIR. |
| **exceed-action** | Define multiple actions for a policy-map class for packets that exceed the CIR. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |

# police aggregate (policy-map class configuration)

Use the **police aggregate** policy-map class configuration command to apply an aggregate policer to multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission, a maximum burst size for transmissions, and an action to take if either maximum is exceeded. Use the **no** form of this command to remove the specified policer.

**police aggregate** *aggregate-policer-name*

**no police aggregate** *aggregate-policer-name*

## Syntax Description

| | |
|---|---|
| *aggregate-policer-name* | Name of the aggregate policer. |

## Defaults

No aggregate policers are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switch supports a maximum of 229 policer instances associated with ports (228 user-configurable policers and 1 policer reserved for internal use). You can configure up to 46 policers on a port.

Aggregate policing applies only to input policy maps.

An aggregate policer differs from an individual policer in that it is shared by multiple traffic classes within a policy map. You use an aggregate policer to police traffic streams across multiple classes in a policy map attached to an interface. You cannot use aggregate policing to aggregate traffic streams across multiple interfaces.

Only one policy map can use any specific aggregate policer.

## Examples

This example shows how to configure the aggregate policing with default actions and apply it across all classes on the same port:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class in-class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class in-class2
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class in-class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show aggregate policer** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policer aggregate** | Displays the aggregate policer configuration. |

# policer aggregate (global configuration)

Use the **policer aggregate** global configuration command to create an aggregate policer to police all traffic across multiple classes in an input policy map. An aggregate policer can be shared by multiple classes in the same policy map. A policer defines a maximum permissible rate of transmission or committed information rate, a maximum burst size for transmissions, and an action to take if the maximum is met or exceeded. Use the **no** form of this command to remove the specified policer.

**policer aggregate** *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [**bc** *burst- value*] [**conform-action** [**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

**no policer aggregate** *aggregate-policer-name* {*rate-bps* | **cir** *cir-bps*} [**bc** *burst- value*] [**conform-action** [**set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**] [**exceed action** [**drop** | **set-cos-transmit** {*new-cos-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-dscp-transmit** {*new-dscp-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-prec-transmit** {*new-precedence-value* | [**cos** | **dscp** | **precedence**] [**table** *table-map name*]} | **set-qos-transmit** *qos-group-value* | **transmit**]]

## Syntax Description

| | |
|---|---|
| *aggregate-policer-name* | Name of the aggregate policer. |
| *rate-bps* | Specify the average traffic rate in bits per second (bps). The range is 8000 to 1000000000. |
| **cir** *cir-bps* | Committed information rate (CIR) in bits per second. The range is 8000 to 1000000000 bps. |
| **bc** *burst- value* | (Optional) Conform burst. The number of acceptable burst bytes. The range is 8000 to 1000000 bytes. If no burst value is entered, the system calculates a burst value that equals the number of bytes that can be sent in 250 milliseconds (ms) at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications. |
| **conform-action** | (Optional) Action to be taken on packets that conform to the CIR. |
| **set-cos-transmit** *cos-value* | Set a new class of service (CoS) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new CoS value is 0 to 7. |
| **set-dscp-transmit** *dscp-value* | Set a new Differentiated Services Code Point (DSCP) value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new DCSP value is 0 to 63. |
| **set-prec-transmit** *precedence-value* | Set a new IP precedence value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new IP precedence value is 0 to 7. |

| | |
|---|---|
| **set-qos-transmit** *qos-group-value* | Set a new quality of service (QoS) group value for the packet and send the packet. This specifies the *to-type* of the marking action. The range for the new QoS value is 0 to 99. |
| **cos** | (Optional) Set the packet marking specified in the preceding keyword based on the CoS value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **dscp** | (Optional) Set the packet marking specified in the preceding keyword based on the DSCP value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **precedence** | (Optional) Set the packet marking specified in the preceding keyword based on the IP precedence value of the incoming packet, and send the packet. This specifies the *from-type* of the enhanced packet-marking action. |
| **table** *table-map name* | (Optional) Used in conjunction with the preceding *from-type* keyword. Specify the table map to be used for the enhanced packet marking. The *to-type* of the action is marked based on the *from-type* parameter of the action using this table map. |
| **transmit** | (Optional) Send the packet unmodified. |
| **exceed action** | (Optional) Action to be taken on packets that do not conform to the CIR. |
| **drop** | Drop the packet. |

## Defaults

No aggregate policers are defined.

When you configure an aggregate policer, conform burst (**bc**) is automatically configured at 250 ms at the configured CIR.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Increased support for configuring conform and exceed actions. See “Usage Guidelines.” |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure conform-action marking using enhanced packet marking and configure exceed-action to send the packet unmodified, perform marking using explicit values, and use all combinations of enhanced packet marking. Enhanced packet marking provides the ability to modify a QoS marking based on any incoming QoS marking and table maps. This release also added support for the ability to mark multiple QoS parameters for the same class, and configure conform-action marking and exceed-action marking simultaneously.

The switch supports a maximum of 256 unique aggregate policer.s.

Aggregate policing is supported only in input policy maps.

You can configure multiple conform and exceed actions simultaneously for an aggregate policer as parameters in the **policer aggregate** global configuration command, but you must enter the actions in this order:

- **conform-action** must be followed by **transmit** or by **set** actions in this order:

  **set-qos-transmit**

  **set-dscp-transmit** or **set-prec-transmit**

  **set-cos-transmit**

- **exceed-action** must be followed by **drop** or **transmit** or by **set** actions in this order:

  **set-qos-transmit**

  **set-dscp-transmit** or **set-prec-transmit**

  **set-cos-transmit**

An output policy map should match only the modified values of the out-of-profile traffic and not the original values.

When you configure an aggregate policer, you can configure specific burst sizes and conform and exceed actions. If burst size (**bc**) is not specified, the system calculates an appropriate burst size value that equals the number of bytes that can be sent in 250 ms at the CIR rate. In most cases, the automatically calculated value is appropriate; enter a new value only if you are aware of all implications.

## Examples

This example shows how to configure an aggregate policer named *agg-pol-1* and attach it to multiple classes within a policy map:

```
Switch(config)# policer aggregate agg-pol-1 10900000 80000 exceed-action drop
Switch(config)# class-map test1
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# class-map test2
Switch(config-cmap)# match access-group 2
Switch(config-cmap)# exit
Switch(config)# policy map testexample
Switch(config-pmap)# class test1
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-cmap-c)# exit
Switch(config-pmap)# class test2
Switch(config-pmap-c)# police aggregate agg-pol-1
Switch(config-pmap-c)# exit
Switch(config-9map)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy input testexample
Switch(config-if)# exit
```

You can verify your settings by entering the **show aggregate-policer** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policer aggregate** | Displays the aggregate policer configuration. |

# policer cpu uni

Use the **policer cpu uni** global configuration command to configure the CPU policing threshold for all user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch. Use the **no** form of this command to return to the default.

**policer cpu uni** *rate-bps*

**no policer cpu uni**

## Syntax Description

| | |
|---|---|
| *rate-bps* | Specify the CPU policing threshold in bits per second (bps). The range is 8000 to 409500. |

## Defaults

The default policing threshold is 160000 bps.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To protect against accidental or intentional CPU overload, the Cisco ME switch automatically provides control-plane security by dropping or rate-limiting a predefined set of Layer 2 control packets and some Layer 3 control packets for UNIs and ENIs. The switch pre-allocates 27 control-plane security policers for CPU protection, numbered 0 to 26. A policer of 26 means a drop policer. A policer of a value of 0 to 25 means that a rate-limiting policer is assigned to the port for the control protocol.

CPU policers are pre-allocated. You can configure only the rate-limiting threshold by using the **policer cpu uni** *rate-bps* command. The configured threshold applies to all control protocols and all UNIs and ENIs.

For more information about control-plane security, see the software configuration guide for this release.

## Examples

This example shows how to set CPU protection threshold to 10000 bps and to verify the configuration.

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# policer cpu uni 10000
Switch(config)# end
```

You can verify your settings by entering the **show policer cpu uni-eni rate** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show policer cpu uni-eni rate** | Displays configured policer threshold for control-plane security. |

# policy-map

Use the **policy-map** global configuration command to create or to modify a policy map that can be attached to multiple physical ports and to enter policy-map configuration mode. Use the **no** form of this command to delete an existing policy map.

**policy-map** *policy-map-name*

**no policy-map** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Name of the policy map. |

## Defaults

No policy maps are defined. By default, packets are sent unmodified.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switch supports a maximum of 256 unique policy maps.

Before configuring policies for classes whose match criteria are defined in a class map, use the **policy-map** command to specify the name of the policy map to be created or modified. Entering the **policy-map** command also enables the policy-map configuration mode, in which you can configure or modify the class policies for that policy map.

After entering the **policy-map** command, you enter policy-map configuration mode, and these configuration commands are available:

- **class**: the specified traffic classification for which the policy actions are applied. The classification is defined in the **class-map** global configuration command. For more information, see the **class-map** command.
- **description**: describes the policy map (up to 200 characters).
- **exit**: exits policy-map configuration mode and returns to global configuration mode.
- **no**: removes a previously defined policy map.

You can configure class policies in a policy map only if the classes have match criteria defined for them. To configure the match criteria for a class, use the **class-map** global configuration and **match** class-map configuration commands. You define packet classification on a physical-port basis.

You can create input policy maps and output policy maps, and you can assign one input policy map and one output policy map to a port. The input policy map acts on incoming traffic on the port; the output policy map acts on outgoing traffic.

You can apply the same policy map to multiple physical ports.

Follow these guidelines when configuring input policy maps:

- The total number of input policy maps that can be attached to interfaces on the switch is limited by the availability of hardware resources. If you attempt to attach an input policy map that would exceed any hardware resource limitation, the configuration fails.
- An input policy map can contain a maximum of 32 class maps, one of which is **class-default**.
- You cannot configure an IP (IP standard and extended ACL, DSCP or IP precedence) and a non-IP (MAC ACL or CoS) classification within the same policy map, either within a single class map or across class maps within the policy map.
- After you use the **service-policy input** policy-map configuration command to attach an input policy map to an interface, you can modify the policy without detaching it from the interface. You can add or delete classification criteria, classes, or actions, or change the parameters of the configured actions (policers, rates, mapping, marking, and so on).
- These commands are not supported on input policy maps: **match qos-grou**p command, **bandwidth** command for Class-Based-Weighting-Queuing (CBWFQ), **priority** command for class-based priority queueing, **queue-limit** command for Weighted Tail Drop (WTD), **shape average** command for port shaping, or class-based traffic shaping.

Follow these guidelines when configuring output policy maps:

- Output policy maps can have a maximum of four classes, one of which is the **class-default**.
- Beginning with Cisco IOS Release 12.2(35)SE, the switch supports configuration and attachment of a unique output policy map for each port on the switch. However, these output policy maps can contain only three configurations of queue limits. You can include these three unique queue-limit configurations in as many output policy maps as there are switch ports. If you try to attach an output policy map that has a fourth queue-limit configuration, you see an error message, and the attachment is not allowed. There are no limitations on the configurations of bandwidth, priority, or shaping.
- All output policy maps must include the same number of class maps (one to three) and the same classification (that is, the same class maps).
- After you have attached a output policy map to an interface by using the **service-policy output** interface configuration command, you can only change the parameters of the configured actions (rates, percentages, and so on) or add or delete classification criteria of the class map while the policy map is attached to the interface. To add or delete a class or an action, you must detach the policy map from all interfaces, change it, and then reattach it to interfaces.
- These commands are not supported on output policy maps: **match access-group** command, **set** command for marking, and **police** command for policing without including the **priority** command.

For more information about policy maps, see the software configuration guide for this release.

## Examples

This example shows how to create an input policy map for three classes:

```
Switch(config)# policy-map input-all
Switch(config-pmap)# class gold
Switch(config-pmap-c)# set dscp af43
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
```

This example shows how to configure an output policy map that provides priority with rate limiting to the gold class and guarantees a minimum remaining bandwidth percent of 20 percent to the silver class and 10 percent to the bronze class:

```
Switch(config)# policy-map output-2
Switch(config-pmap)# class gold-out
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver-out
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze-out
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# exit
```

This example shows how to delete the policy map *output-2*:

```
Switch(config)# no policy-map output-2
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **service-policy (interface configuration)** | Applies a policy map to a port. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |

# port-channel load-balance

Use the **port-channel load-balance** global configuration command to set the load-distribution method among the ports in the EtherChannel. Use the **no** form of this command to return to the default setting.

**port-channel load-balance** {**dst-ip** | **dst-mac** | **src-dst-ip** | **src-dst-mac** | **src-ip** | **src-mac**}

**no port-channel load-balance**

## Syntax Description

| | |
|---|---|
| **dst-ip** | Load distribution is based on the destination host IP address. |
| **dst-mac** | Load distribution is based on the destination host MAC address. Packets to the same destination are sent on the same port, but packets to different destinations are sent on different ports in the channel. |
| **src-dst-ip** | Load distribution is based on the source and destination host IP address. |
| **src-dst-mac** | Load distribution is based on the source and destination host MAC address. |
| **src-ip** | Load distribution is based on the source host IP address. |
| **src-mac** | Load distribution is based on the source MAC address. Packets from different hosts use different ports in the channel, but packets from the same host use the same port. |

## Defaults

The default is **src-mac**.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For information about when to use these forwarding methods, see the "Configuring EtherChannels" chapter in the software configuration guide for this release.

## Examples

This example shows how to set the load-distribution method to **dst-mac**:

```
Switch(config)# port-channel load-balance dst-mac
```

You can verify your setting by entering the **show running-config** privileged EXEC command or the **show etherchannel load-balance** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **interface port-channel** | Accesses or creates the port channel. |
| **show etherchannel** | Displays EtherChannel information for a channel. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# port-type

Use the **port-type** interface configuration command to change the port type on a Cisco ME switch from its existing port type to a network node interface (NNI), a user network interface (UNI), or an enhanced network interfaces (ENI). Use the **no** form of this command to return the port to its default setting.

**port-type** {**eni** | **nni** | **uni**}

**no port-type**

## Syntax Description

| | |
|---|---|
| **eni** | Enhanced network interface. ENIs have the same default configuration as UNIs, but you can configure ENI to support protocol control packets for Cisco Discovery Protocol (CDP), Spanning-Tree Protocol (STP), Link Layer Discovery Protocol (LLDP), and EtherChannel Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP). |
| **nni** | Network node interface. |
| **uni** | User network interface. |

## Defaults

If no configuration file exists, all the 10/100 ports on the Cisco ME switch are UNIs, and the small form-factor pluggable (SFP) module slots on the Cisco ME switch are NNIs. You must configure a port to be an ENI port.

A port configured as an ENI has the same defaults as a UNI port, but the you can configure control protocols (CDP, STP, LLDP, LACP and PAgP) on ENIs. These protocols are not supported on UNIs.

The default status for a UNI or ENI is administratively down to prevent unauthorized users from gaining access to other ports as you configure the switch. You must use the **no shutdown** interface configuration command to enable a UNI or ENI before you can configure it.

The default status for an NNI is administratively up to allow a service provider remote access to the switch during initial configuration.

Configuring a port as an ENI does not change the administrative state of the port. If the port state is **shutdown** before a port-type change, it remains in **shutdown** state; if the state is **no shutdown**, it remains in **no shutdown** state.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(44)SE | The **eni** keyword was added. |

## Usage Guidelines

A port can be reconfigured to another port type. When a port is reconfigured as the other interface type, it inherits all the characteristics of that interface type. By default all ports on the switch are either UNI or NNI. At any time, all ports on the Cisco ME switch are UNIs, NNIs, or ENIs.

Some features are not supported only on all port types. Control protocols (CDP, STP, LLDP, and EtherChannel LACP and PAgP) have different support on each port type:

- On NNIs, these features are enabled by default.
- On ENIs, these features are disabled by default, but you can enable them by using the command-line interface.
- On UNIs, these features are not supported.

For information about specific feature support, see the software configuration guide for this release.When you change a port from one type to another, any features exclusive to a port type are removed from the configuration to prevent conflicting configuration options on a specific interface.

Every port on the switch can be a UNI or ENI, but only four ports can be NNIs at the same time. When you use the **no port-type** command on any interface, whether it is currently a UNI, ENI, or NNI, the interface defaults to UNI.

Traffic is not switched between UNIs or ENIs, and all traffic incoming on UNIs or ENIs must exit on NNIs to prevent a user from gaining access to another user's private network. If it is appropriate for two or more UNIs or ENIs to exchange traffic within the switch, you can assign the interface to a community VLAN. A community VLAN can contain a maximum of eight UNIs or ENIs. We do not recommend mixing UNIs and ENIs in the same community VLAN.

For more information about configuring VLANs, see the software configuration guide for this release.

## Examples

This example shows how to change a port to an NNI.

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type nni
5d20h: %SYS-5-CONFIG_I: Configured from console by console
Switch(config-if)# end
Switch# copy running-config startup-config
```

This example shows how to change a port type to an ENI.

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface fastethernet0/1
Switch(config-if)# no shutdown
Switch(config-if)# port-type eni
Switch(config-if)# end
```

## Related Commands

| Command | Description |
|---|---|
| **no shutdown** | Enables an interface. |
| **show interfaces** | Displays the statistical information specific to all interfaces or to a specific interface. |
| **show port-type** | Displays the port type of an interface. |

# priority

Use the **priority** policy-map class configuration command to configure class-based priority queuing for a class of traffic belonging to an output policy map. The switch supports strict priority queuing or priority used with the **police** policy-map command. Use the **no** form of this command to remove a priority specified for a class.

**priority**

**no priority**

**Note** When the **police** command is used with the **priority** policy-map class command for unconditionally rate-limiting the priority queue, burst size values are not supported for the **police** command.

## Syntax Description

This command has no arguments or keywords.

## Defaults

No policers are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When used by itself (not followed by the **police** policy-map command), the **priority** command assigns traffic to a low-latency path and ensures that packets belonging to the class have the lowest possible latency. With strict priority queuing, packets in the priority queue are scheduled and sent until the queue is empty.

**Note** You should exercise care when using the **priority** command without the **policy** command. Excessive use of strict priority queuing might cause congestion in other queues.

You can use **priority** with the **police** {*rate-bps* | **cir** *cir-bps*} policy-map command to reduce the bandwidth used by the priority queue. This is the only form of policing that is supported in output policy maps. Using this combination of commands configures a maximum rate on the priority queue and allows you to use the **bandwidth** and **shape average** policy-map commands for other classes to allocate traffic rates on other queues.

**Note** When you use the **police** command with the **priority** command in an output policy, the police rate range is 64000 to 1000000000 bps, even though the range that appears in the command-line help is 8000 to 1000000000. Configured burst size is ignored when you try to attach the output service policy.

When you configure priority in an output policy map without the **police** command, you can only configure the other queues for sharing by using the **bandwidth remaining percent** policy-map class command. This command does not guarantee the allocated bandwidth, but the rate of distribution.

When you configure priority in an output policy map with the **police** command, you can configure other queues for sharing by using the **bandwidth** policy-map class command and for shaping by using the **shape average** policy-map class command.

You can associate the **priority** command only with a single unique class for all attached output policies on the switch.

You cannot associate the **priority** command with the **class-default** of the output policy map.

You cannot configure priority and any other scheduling action (**shape average** or **bandwidth**) in the same class.

The **priority** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default set by the **priority** command.

## Examples

This example shows how to configure the class *out-class1* as a strict priority queue so that all packets in that class are sent before any other class of traffic. Other traffic queues are configured so that *out-class-2* gets 50 percent of the remaining bandwidth and *out-class3* gets 20 percent of the remaining bandwidth. The class **class-default** receives the remaining 30 percent with no guarantees.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth remaining percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth remaining percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

This example shows how to use the **priority** with **police** commands to configure *out-class1* as the priority queue, with traffic going to the queue limited to 20000000 bits per second (bps) so that the priority queue never uses more than that. Traffic above that rate is dropped. The other traffic queues are configured as in the previous example.

```
Switch(config)# policy-map policy1
Switch(config-pmap)# class out-class1
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# police 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class2
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# exit
Switch(config-pmap)# class out-class3
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet0/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **police** | Defines a policer for classified traffic. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |

# private-vlan

Use the **private-vlan** VLAN configuration command to configure private VLANs and to configure the association between private-VLAN primary and secondary VLANs. Use the **no** form of this command to return the VLAN to normal VLAN configuration.

**private-vlan** {**association** [**add** | **remove**] *secondary-vlan-list* | **community** | **isolated** | **primary**}

**no private-vlan** {**association** | **community** | **isolated** | **primary**}

## Syntax Description

| | |
|---|---|
| **association** | Create an association between the primary VLAN and a secondary VLAN. |
| *secondary-vlan-list* | Specify one or more secondary VLANs to be associated with a primary VLAN in a private VLAN. |
| **add** | Associate a secondary VLAN to a primary VLAN. |
| **remove** | Clear the association between a secondary VLAN and a primary VLAN. |
| **community** | Designate the VLAN as a community VLAN. |
| **isolated** | Designate the VLAN as a community VLAN. |
| **primary** | Designate the VLAN as a community VLAN. |

## Defaults

The default is to no configured private VLANs.

## Command Modes

VLAN configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You must manually configure private VLANs on all switches in the Layer 2 network to merge their Layer 2 databases and to prevent flooding of private-VLAN traffic.

You cannot include VLAN 1 or VLANs 1002 to 1005 in the private-VLAN configuration. Extended VLANs (VLAN IDs 1006 to 4094) can be configured as private VLANs.

You can **associate** a secondary (isolated or community) VLAN with only one primary VLAN. A primary VLAN can have one isolated VLAN and multiple community VLANs associated with it.

- A secondary VLAN cannot be configured as a primary VLAN.
- The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.
- If you delete either the primary or secondary VLANs, the ports associated with the VLAN become inactive.

A **community** VLAN carries traffic among community ports and from community ports to the promiscuous ports on the corresponding primary VLAN. A community VLAN can include no more than eight user network interfaces (UNIs).

An **isolated** VLAN is used by isolated ports to communicate with promiscuous ports. It does not carry traffic to other community ports or to isolated ports with the same primary VLAN domain.

A **primary** VLAN is the VLAN that carries traffic from a gateway to customer end stations on private ports.

The **private-vlan** commands do not take effect until you exit from VLAN configuration mode.

Do not configure private-VLAN ports as EtherChannels. While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

A private VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A private VLAN cannot be a user network interface-enhanced network interface (UNI-ENI) VLAN. If the VLAN is a UNI-ENI isolated VLAN (the default), you can change it to a private VLAN by entering the **private-vlan** VLAN configuration command. If a VLAN has been configured as a UNI-ENI community VLAN, you must first enter the **no uni-vlan** VLAN configuration command before configuring it as a private VLAN.

Although a private VLAN contains more than one VLAN, only one STP instance runs for the entire private VLAN. When a secondary VLAN is associated with the primary VLAN, the STP parameters of the primary VLAN are propagated to the secondary VLAN.

See the **switchport private-vlan** command for information about configuring host ports and promiscuous ports.

**Note** For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

## Examples

This example shows how to configure VLAN 20 as a primary VLAN, VLAN 501 as an isolated VLAN, VLANs 502 and 503 as community VLANs, and to associate them in a private VLAN. The example assumes that VLANs 502 and 503 were previously configured as UNI-ENI community VLANs.

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 501
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 502
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 503
Switch(config-vlan)# no uni-vlan
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# exit
Switch(config)# vlan 20
Switch(config-vlan)# private-vlan association 501-503
Switch(config-vlan)# end
```

You can verify your setting by entering the **show vlan private-vlan** or **show interfaces status** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces status** | Displays the status of interfaces, including the VLANs to which they belong. |
| **show vlan private-vlan** | Displays the private VLANs and VLAN associations configured on the switch. |
| **switchport private-vlan** | Configures a private-VLAN port as a host port or promiscuous port. |

# queue-limit

Use the **queue-limit** policy-map class configuration command to set the queue maximum threshold for Weighted Tail Drop (WTD) in an output policy map. Use the **no** form of this command to return to the default.

**queue-limit** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]

**no queue-limit** [**cos** *value* | **dscp** *value* | **precedence** *value* | **qos-group** *value*] *number-of-packets* [**packets**]

## Syntax Description

| | |
|---|---|
| **cos** *value* | (Optional) Set the parameters for each cost of service (CoS) value. The range is from 0 to 7. |
| **dscp** *value* | (Optional) Set the parameters for each Differentiated Services Code Point (DSCP) value. The range is from 0 to 63. |
| **precedence** *value* | (Optional) Set the parameters for each IP precedence value. The range is from 0 to 7. |
| **qos-group** *value* | (Optional) Set the parameters for each quality-of-service (QoS) group value. The range is from 0 to 99. |
| *number-of-packets* [**packets**] | Set the maximum threshold for WTD as the number of packets in the queue. The range is from 16 to 544 and refers to 256-byte packets. The default is 48 packets. The **packets** keyword is optional.<br>**Note** For optimal network performance, we strongly recommend that you configure the maximum queue-limit to 272 or less. |

## Defaults

Default queue limit is 48 (256-byte) packets.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.25(SEG) | Support was added to configure the **queue-limit** in the **class-default** of an output policy map. |

## Usage Guidelines

You use the **queue-limit** policy-map class command to control output traffic. Queue-limit settings are not supported in input policy maps.

Beginning with Cisco IOS Release 12.2(35)SE, the switch supports one output policy map for each interface. However the limit of three unique queue-limit configurations across all output policy maps remains in effect You can use the same queue-limit configuration across multiple policy maps.

Within an output policy map only four queues (classes) are allowed, including the class default. Each queue has three defined thresholds (queue limits). Only three queue-limit configurations are allowed on the switch, but multiple policy maps can share the same queue-limits. For two policy maps to share a queue-limit configuration, all threshold values must be the same for all classes in both policy maps.

If you try to attach an output policy map that contains a fourth queue-limit configuration to an interface, you see an error message and the attachment is not allowed.

The **queue-limit** command is supported only after you first configure a scheduling action, such as **bandwidth**, **shape-average**, or **priority**, except when you configure **queue-limit** in the **class-default** of an output policy map.

You cannot configure more than two unique threshold values for WTD qualifiers (**cos**, **dscp**, **precedence**, or **qos-group**) in the **queue-limit** command. However, you can map any number of qualifiers to those thresholds. You can configure a third unique threshold value to set the maximum queue, using the **queue-limit** command with no qualifiers.

When you use the **queue-limit** command to configure thresholds within a class map, the WTD thresholds must be less than or equal to the maximum threshold of the queue. This means that the queue size configured without a qualifier must be larger than any of the queue sizes configured with a qualifier.

## Examples

This example shows how to configure WTD so that *out-class1*, *out-class2*, *out-class3*, and **class-default** get a minimum of 40, 20, 10 and 10 percent of the traffic bandwidth respectively. The corresponding queue-sizes are set to 48, 32, 16 and 272 (256-byte) packets:

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 40
Switch(config-pmap-c)# queue-limit 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 272
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

This example shows how to configure WTD for a Fast Ethernet port where *outclass1*, *outclass2*, and *outclass3* get a minimum of 50, 20, and 10 percent of the traffic bandwidth. The **class-default** gets the remaining 20 percent. Each corresponding queue size is set to 64, 32, and 16 (256-byte) packets, respectively. The example also shows how if *outclass1* matches to dscp 46, 56, 57, 58, 60, 63, a DSCP value of 46 gets a queue size of 32 (256-byte) packets; DSCP values 56, 57, and 58 get queue sizes of 48 (256-byte) packets; and the remaining DSCP values of 60 and 63 get the default queue size of 64 (256-byte) packets.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class outclass1
Switch(config-pmap-c)# bandwidth percent 50
Switch(config-pmap-c)# queue-limit 64
Switch(config-pmap-c)# queue-limit dscp 46 32
Switch(config-pmap-c)# queue-limit dscp 56 48
Switch(config-pmap-c)# queue-limit dscp 57 48
Switch(config-pmap-c)# queue-limit dscp 58 48
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass2
Switch(config-pmap-c)# bandwidth percent 20
Switch(config-pmap-c)# queue-limit 32
Switch(config-pmap-c)# exit
Switch(config-pmap)# class outclass3
Switch(config-pmap-c)# bandwidth percent 10
Switch(config-pmap-c)# queue-limit 16
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy output out-policy
Switch(config-if)# exit
```

You can use these same queue-limit values in multiple output policy maps on the switch. However, changing one of the queue-limit values in a class would create a new, unique queue-limit configuration. You can attach only three unique queue-limit configurations in output policy maps to interfaces at any one time. If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |

# remote-span

Use the **remote-span** VLAN configuration command to configure a VLAN as a Remote Switched Port Analyzer (RSPAN) VLAN. Use the **no** form of this command to remove the RSPAN designation from the VLAN.

**remote-span**

**no remote-span**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No RSPAN VLANs are defined.

## Command Modes

VLAN configuration (config-VLAN)

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Valid RSPAN VLAN IDs are 2 to 1001 and 1006 to 4094. The RSPAN VLAN cannot be VLAN 1 (the default VLAN) or VLAN IDs 1002 to 1005 (reserved for Token Ring and FDDI VLANs).

Before you configure the RSPAN **remote-span** command, use the **vlan** global configuration command to create the VLAN.

- To change a VLAN from a user network interface-enhanced network interface (UNI-ENI) isolated VLAN (the default) to an RSPAN VLAN, enter the **rspan-vlan** VLAN configuration command.
- To change a UNI-ENI community VLAN to an RSPAN VLAN, you must first remove the community VLAN type by entering the **no uni-vlan** VLAN configuration command.

The RSPAN VLAN has these characteristics:

- No MAC address learning occurs on it.
- RSPAN VLAN traffic flows only on trunk ports.
- Spanning Tree Protocol (STP) can run in the RSPAN VLAN, but it does not run on RSPAN destination ports. On the Cisco ME switch only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled participate in STP.

You must manually also configure both source, destination, and intermediate switches (those in the RSPAN VLAN between the source switch and the destination switch) with the RSPAN VLAN ID.

When an existing VLAN is configured as an RSPAN VLAN, the VLAN is first deleted and then recreated as an RSPAN VLAN. Any access ports become inactive until the RSPAN feature is disabled.

## Examples

This example shows how to configure a VLAN as an RSPAN VLAN.

```
Switch(config)# vlan 901
Switch(config-vlan)# remote-span
```

This example shows how to remove the RSPAN feature from a VLAN.

```
Switch(config)# vlan 901
Switch(config-vlan)# no remote-span
```

You can verify your settings by entering the **show vlan remote-span** user EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **monitor session** | Enables Switched Port Analyzer (SPAN) and RSPAN monitoring on a port and configures a port as a source or destination port. |
| **vlan** | Changes to config-vlan mode where you can configure VLANs 1 to 4094. |

# renew ip dhcp snooping database

Use the **renew ip dhcp snooping database** privileged EXEC command to renew the DHCP snooping binding database.

**renew ip dhcp snooping database** [**validation none**] [{**flash:/***filename* | **ftp://***user:password@host/filename* | **nvram:/***filename* | **rcp://***user@host/filename* | **tftp://***host/filename*}] [**validation none**]

## Syntax Description

| | |
|---|---|
| **validation none** | (Optional) Specify that the switch does not verify the cyclic redundancy check (CRC) for the entries in the binding file specified by the URL. |
| **flash:/***filename* | (Optional) Specify that the database agent or the binding file is in the flash memory. |
| **ftp://***user***:***password***@***host***/***filename* | (Optional) Specify that the database agent or the binding file is on an FTP server. |
| **nvram:/***filename* | (Optional) Specify that the database agent or the binding file is in the NVRAM. |
| **rcp://***user@host/filename* | (Optional) Specify that the database agent or the binding file is on a Remote Control Protocol (RCP) server. |
| **tftp://***host/filename* | (Optional) Specify that the database agent or the binding file is on a TFTP server. |

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a URL, the switch tries to read the file from the configured URL.

## Examples

This example shows how to renew the DHCP snooping binding database without checking CRC values:

```
Switch# renew ip dhcp snooping database validation none
```

You can verify settings by entering the **show ip dhcp snooping database** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables DHCP snooping on a VLAN. |
| **ip dhcp snooping binding** | Configures the DHCP snooping binding database. |
| **show ip dhcp snooping database** | Displays the status of the DHCP snooping database agent. |

# rmon collection stats

Use the **rmon collection stats** interface configuration command to collect Ethernet group statistics, which include usage statistics about broadcast and multicast packets, and error statistics about cyclic redundancy check (CRC) alignment errors and collisions. Use the **no** form of this command to return to the default setting.

**rmon collection stats** *index* [**owner** *name*]

**no rmon collection stats** *index* [**owner** *name*]

## Syntax Description

| | |
|---|---|
| *index* | Remote Network Monitoring (RMON) collection control index. The range is 1 to 65535. |
| **owner** *name* | (Optional) Owner of the RMON collection. |

## Defaults

The RMON statistics collection is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The RMON statistics collection command is based on hardware counters. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **rmon collection stats** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

## Examples

This example shows how to collect RMON statistics for the owner *root*:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# rmon collection stats 2 owner root
```

You can verify your setting by entering the **show rmon statistics** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show rmon statistics** | Displays RMON statistics.<br>For syntax information, select **Cisco IOS Configuration Fundamentals Command Reference, Release 12.2 > System Management Commands > RMON Commands.** |

# service password-recovery

Use the **service password-recovery** global configuration command to enable the password-recovery mechanism (the default). This mechanism allows an end user with physical access to the switch to press the break key on the console terminal to interrupt the boot process while the switch is powering up and to assign a new password.

Use the **no** form of this command to disable part of the password-recovery functionality. When the password-recovery mechanism is disabled, interrupting the boot process is allowed only if the user agrees to set the system back to the default configuration.

**service password-recovery**

**no service password-recovery**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The password-recovery mechanism is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

As a system administrator, you can use the **no service password-recovery** command to disable some of the functionality of the password recovery feature by allowing an end user to reset a password only by agreeing to return to the default configuration. This provides configuration file security by ensuring that only authenticated and authorized users have access to the configuration file and prevents users from accessing the configuration file by using the password recovery process.

The password recovery procedure requires using a break key. After the switch performs power-on self test (POST), the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 5 seconds *****

Send a break key to prevent autobooting.
```

You must enter the break key on the console terminal within 5 seconds of receiving the message that the system will autoboot. A user with physical access to the switch presses the break key on the console terminal within 5 seconds of receiving the message that flash memory is initializing. The System LED flashes green until the **break key** is accepted. After the **break key** is accepted, the System LED turns off until after the switch boots.

If the password-recovery mechanism is disabled, this message appears:

```
The password-recovery mechanism has been triggered, but
is currently disabled. Access to the boot loader prompt
through the password-recovery mechanism is disallowed at
this point. However, if you agree to let the system be
reset back to the default system configuration, access
to the boot loader prompt can still be allowed.

Would you like to reset the system back to the default configuration (y/n)?
```

If the user chooses not to reset the system to the default configuration, the normal boot process continues as if the **break key** had not been pressed. If you choose to reset the system to the default configuration, the configuration file in flash memory is deleted, and the VLAN database file, *flash:vlan.dat* (if present), is deleted.

**Note** If you use the **no service password-recovery** command to control end user access to passwords, we recommend that you save a copy of the configuration file in a location away from the switch in case the end user uses the password recovery procedure and sets the system back to default values. Do not keep a backup copy of the configuration file on the switch.

You can enter the **show version** privileged EXEC command to determine if password recovery is enabled or disabled.

## Examples

This example shows how to disable password recovery on a switch so that a user can only reset a password by agreeing to return to the default configuration.

```
Switch(config)# no service-password recovery
Switch(config)# exit
```

## Related Commands

| Command | Description |
|---|---|
| show version | Displays version information for the hardware and firmware. |

# service-policy (interface configuration)

Use the **service-policy** interface configuration command to apply a policy map defined by the **policy-map** command to the incoming or outgoing traffic of a physical port. Use the **no** form of this command to remove the policy map and port association.

**service-policy** {**input** | **output**} *policy-map-name*

**no service-policy** {**input** | **output**} *policy-map-name*

## Syntax Description

| | |
|---|---|
| **input** | Apply the policy map to the input of a physical port. |
| **output** | Apply the policy map to the output of a physical port. |
| *policy-map-name* | The specified policy map to be applied. |

**Note** Though visible in the command-line help strings, the **history** keyword is not supported, and you should ignore the statistics that it gathers.

## Defaults

No policy maps are attached to the port.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Only one input policy map and one output policy map can be attached to an interface.

Beginning with Cisco IOS Release 12.2(35)SE, you can attach an output policy map to each interface on the switch. However, the switch supports a limit of three unique queue-limit configurations across all output policy maps at any time. Multiple policy maps can share the same queue-limit configuration.If you try to attach an output policy map with a fourth unique queue-limit configuration, you see this error message:

```
QoS: Configuration failed. Maximum number of allowable unique queue-limit
configurations exceeded.
```

You can attach input or output policy maps to a Fast Ethernet or Gigabit Ethernet port. You cannot attach policy maps to switch virtual interfaces (SVIs) and EtherChannel interfaces.

## Examples

This example shows how to apply *plcmap1* as an output policy map:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# service-policy output plcmap1
```

This example shows how to remove *plcmap2* from the port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no service-policy output plcmap2
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |
| **show policy-map interface** [*interface-id*] | Displays policy maps configured on the specified interface or on all interfaces. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# service-policy (policy-map class configuration)

Use the **service-policy** policy-map class configuration command to configure a quality of service (Q0S) service policy for anoutput policy map. Use the **no** form of this command to disable a service policy as a QoS policy within a policy map.

**service-policy** *policy-map-name*

**no service-policy** *policy-map-name*

## Syntax Description

| | |
|---|---|
| *policy-map-name* | Name of the service policy map (created by using the **policy-map** global configuration command) to be used in a QoS hierarchical service policy. |

## Defaults

No service policies are defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You attach a service policy created in policy-map class configuration to a parent output policy map. This creates hierarchical policy mapping. Use the **service-policy** *policy-map-name* policy-map class configuration command to enter a second-level (child) policy map.

For an output policy map, when **shape average** is also configured on the class **class-default**, you can configure hierarchical policy maps by attaching a single **service-policy** policy-map class command to the class **class-default**. This policy map specifies the service policy for the port-shaped traffic on the port and is the parent policy map. You can configure the child policy with class-based queuing actions by using the **queue-limit** policy map class command and with scheduling actions (by using the **bandwidth**, **shape average**, or **priority** command).

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to define the service policy and to attach it to a parent policy map to set the maximum bandwidth (shape) for an output queue at 90000000 bits per second:

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays quality of service (QoS) policy maps. |

# set cos

Use the **set cos** policy-map class configuration command to set a Layer 2 class of service (CoS) value in the packet. Use the **no** form of this command to remove traffic marking.

**set cos** {*cos_value* | *from-field* [**table** *table-map-name*]}

**no set cos** {*cos_value* | *from-field* [**table** *table-map-name*]}

## Syntax Description

| | |
|---|---|
| *cos_value* | Enter an IEEE 802.1Q class of service/user priority value with which to classify traffic. The range is from 0 to 7. |
| *from-field* | Specific a packet-marking category to be used to set the CoS value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category.<br>These options are supported:<br>• **cos**—CoS value<br>• **dscp**—Differentiated Services Code Point (DSCP) value.<br>• **precedence**—IP-precedence value |
| **table** | (Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the CoS value |
| *table-map-name* | (Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the CoS value. The table map name can be a maximum of 64 alphanumeric characters. |

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12-2(25)SEG | Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.” |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set cos** with all other marking actions, specifically **set dscp**, **set precedence**, and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use the **set cos** command if you want to mark a packet that is being sent to a switch. Switches can leverage Layer 2 header information including a CoS value marking.

You can use the **match cos** class-map configuration command and the **set cos** policy-map class configuration command together to allow switches to interoperate and provide quality of service (QoS) based on the CoS markings. You can also configure Layer 2 to Layer 3 mapping by matching on the CoS value because switches can already match and set CoS values.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the CoS value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the CoS value. For example, if you enter the **set cos precedence** command, the precedence value is copied and used as the CoS value. If you enter the **set cos dscp** command, the DSCP value is copied and used as the CoS value.

## Examples

This example shows how to set all FTP traffic to cos 3:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set cos 3
Switch(config-pmap-c)# exit
```

This example shows how to assign a DSCP to CoS table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos dscp table dscp-cos-tablemap
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |

# set dscp

Use the **set** [**ip**] **dscp** policy-map class configuration command to mark IPv4 traffic by setting a Differentiated Services Code Point (DSCP) value in the type of service (ToS) byte of the packet. Use the **no** form of this command to remove traffic marking.

**set** [**ip**] **dscp** {*dscp_value* |*from-field* [**table** *table-map-name*]}

**no set** [**ip**] **dscp** {*dscp_value* | *from-field* [**table** *table-map-name*]}

**Note** Entering **ip dscp** is the same as entering **dscp**.

## Syntax Description

| | |
|---|---|
| *dscp-value* | Enter a DSCP value with which to classify traffic. The range is from 0 to 63. You also can enter a mnemonic name for a commonly used value. |
| *from-field* | Specific a packet-marking category to be used to set the DSCP value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category.<br>These options are supported:<br>• **cos**—class of service (CoS) value<br>• **dscp**—DSCP value.<br>• **precedence**—IP-precedence value |
| **table** | (Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the DSCP value |
| *table-map-name* | (Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the DSCP value. The table map name can be a maximum of 64 alphanumeric characters. |

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12-2(25)SEG | Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.” |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set dscp** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set dscp** command with the **set precedence** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After DSCP bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the DSCP value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the DSCP value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the DSCP value. For example, if you enter the **set dscp cos** command, the CoS value is copied and used as the DSCP value.

## Examples

This example shows how to set all FTP traffic to DSCP 10:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set dscp 10
Switch(config-pmap-c)# exit
```

This example shows how to assign a CoS to DSCP table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table cos-dscp-tablemap
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |

# set precedence

Use the **set** [**ip**] **precedence** policy-map class configuration command to mark IPv4 traffic by setting an IP-precedence value in the packet. Use the **no** form of this command to remove traffic marking.

**set** [**ip**] **precedence** {*precedence_value* | *from-field* [**table** *table-map-name*]}

**no set** [**ip**] **precedence** {*precedence_value* | *from-field* [**table** *table-map-name*]}

**Note** Entering **ip precedence** is the same as entering **precedence**.

## Syntax Description

| | |
|---|---|
| *precedence_value* | Enter an IPv4 precedence value with which to classify traffic. The range is 0 to 7. You also can enter a mnemonic name for a commonly used value. |
| *from-field* | Specific a packet-marking category to be used to set the precedence value of the packet. If you are using a table map for mapping and converting packet-marking values, this establishes the *map-from* packet-marking category.<br>These options are supported:<br>• **cos**—class of service (CoS) value<br>• **dscp**—Differentiated Services Code Point (DSCP) value.<br>• **precedence**—IP-precedence value |
| **table** | (Optional) Used in conjunction with the *from-field* keyword. Indicates that the values set in a specified table map are used to set the precedence value |
| *table-map-name* | (Optional) Used in conjunction with the **table** keyword. Name of the table map used to specify the precedence value. The table map name can be a maximum of 64 alphanumeric characters. |

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12-2(25)SEG | Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See “Usage Guidelines.” |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set precedence** with other marking actions, specifically **set cos** and **set qos-group**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

You cannot use the **set precedence** command with the **set dscp** command to mark the same packet. DSCP values and IP precedence values are mutually exclusive. A packet can have one value of the other, but not both.

After precedence bits are set, other quality of service (QoS) features can then operate on the bit settings.

The network gives priority (or some type of expedited handling) to marked traffic. Typically, you set the precedence value at the edge of the network (or administrative domain) and data is then queued according to the precedence. Class-based weighted fair queuing (CBWFQ) can speed up handling for high-precedence traffic at congestion points. Weighted Tail Drop (WTD) ensures that high-precedence traffic has lower loss rates than other traffic during times of congestion.

Instead of using numeric values, you can also specify the *dscp-value* by using the reserved keywords **EF**, **AF11**, and **AF12**.

If you are using this command to perform enhanced packet marking, you can use the *from-field* packet marking option for mapping and setting the precedence value. The supported *from-field* marking categories are: CoS, DSCP, and IP precedence.

If you specify a *from-field* category, but do not specify the **table** keyword and *table-map-name,* the default action is to copy the value associated with the *from-field* category as the precedence value. For example, if you enter the **set precedence cos** command, the CoS value is copied and used as the precedence value.

## Examples

This example shows how to give all FTP traffic an IP precedence value of 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set precedence 5
Switch(config-pmap-c)# exit
```

This example shows how to assign a CoS to precedence table map to a class:

```
Switch(config)# policy-map inpolicy
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table cos-prec-tablemap
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |

# set qos-group

Use the **set qos-group** policy-map class configuration command to set a a quality of service (QoS) group identifier that can be used later to classify packets. Use the **no** form of this command to remove the group identifier.

**set qos-group** *value*

**no set qos-group** *value*

## Syntax Description

| | |
|---|---|
| *value* | Set the QoS group value to use to classify traffic. The range is from 0 to 99. |

## Defaults

No traffic marking is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The number of supported QoS groups was increased to 100. Support was added to set multiple marking actions and to use table maps for enhanced packet marking. See "Usage Guidelines." |

## Usage Guidelines

Beginning with Cisco IOS Release 12.2(25)SEG, you can configure **set qos-group** with all other marking actions, specifically **set cos, set dscp**, and **set precedence**, for the same class. Support was also added for the ability to configure more than one marking action with enhanced packet marking by using table maps for the same class.

Use this command to associate a QoS group value with a traffic flow as it enters the switch, which can then be used in an output policy map to identify the flow.

A maximum of 100 QoS groups (0 through 99) is supported on the switch.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to set all FTP traffic to QoS group 5:

```
Switch(config)# policy-map policy_ftp
Switch(config-pmap)# class ftp_class
Switch(config-pmap-c)# set qos-group 5
Switch(config-pmap-c)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| class | Defines a traffic classification match criteria for the specified class-map name. |
| policy-map | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| show policy-map | Displays QoS policy maps. |

# setup

Use the setup privileged EXEC command to configure the switch with its initial configuration.

**setup**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you use the **setup** command, make sure that you have this information:

- IP address and network mask
- Password strategy for your environment

When you enter the **setup** command, an interactive dialog, called the System Configuration Dialog, appears. It guides you through the configuration process and prompts you for information. The values shown in brackets next to each prompt are the default values last set by using either the **setup** command facility or the **configure** privileged EXEC command.

Help text is provided for each prompt. To access help text, press the question mark (**?**) key at a prompt.

To return to the privileged EXEC prompt without making changes and without running through the entire System Configuration Dialog, press **Ctrl-C**.

When you complete your changes, the setup program shows you the configuration command script that was created during the setup session. You can save the configuration in NVRAM or return to the setup program or the command-line prompt without saving it.

## Examples

This is an example of output from the **setup** command:

```
Switch# setup
--- System Configuration Dialog ---

Continue with configuration dialog? [yes/no]: yes

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Basic management setup configures only enough connectivity
for management of the system, extended setup will ask you
to configure each interface on the system.

Would you like to enter basic management setup? [yes/no]: yes
Configuring global parameters:
```

```
Enter host name [Switch]:host-name

  The enable secret is a password used to protect access to
  privileged EXEC and configuration modes. This password, after
  entered, becomes encrypted in the configuration.
  Enter enable secret: enable-secret-password

  The enable password is used when you do not specify an
  enable secret password, with some older software versions, and
  some boot images.
  Enter enable password: enable-password

  The virtual terminal password is used to protect
  access to the router over a network interface.
  Enter virtual terminal password: terminal-password

  Configure SNMP Network Management? [no]: yes
  Community string [public]:

Current interface summary
Any interface listed with OK? value "NO" does not have a valid configuration

Interface                  IP-Address      OK? Method Status                Protocol
Vlan1                      172.20.135.202  YES NVRAM  up                    up

GigabitEthernet0/1         unassigned      YES unset  up                    up

GigabitEthernet0/2         unassigned      YES unset  up                    down

<output truncated>

Port-channel1              unassigned      YES unset  up                    down

Enter interface name used to connect to the
management network from the above interface summary: vlan1

Configuring interface vlan1:
Configure IP on this interface? [yes]: yes
IP address for this interface: ip_address
Subnet mask for this interface [255.0.0.0]: subnet_mask

The following configuration command script was created:

hostname host-name
enable secret 5 $1$LiBw$0Xc1wyT.PXPkuhFwqyhVi0
enable password enable-password
line vty 0 15
password terminal-password
snmp-server community public
!
no ip routing
!
interface GigabitEthernet0/1
no ip address
!
interface GigabitEthernet0/2
no ip address
!
end
```

```
Use this configuration? [yes/no]: yes
!
[0] Go to the IOS command prompt without saving this config.

[1] Return back to the setup without saving this config.

[2] Save this configuration to nvram and exit.

Enter your selection [2]:
```

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **show version** | Displays version information for the hardware and firmware. |

# shape average

Use the **shape average** policy-map class configuration command to configure class-based shaping by specifying the average traffic shaping rate. Use the command with the class **class-default** to set port shaping. Use the **no** form of this command to remove traffic shaping.

**shape average** *target bps*

**no shape average** *target bps*

## Syntax Description

| | |
|---|---|
| *target bps* | Target average bit rate in bits per second (bps). The range is from 64000 to 1000000000. |

## Defaults

No traffic shaping is defined.

## Command Modes

Policy-map class configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | Support was added to configure traffic shaping in the **class-default** of an output policy map. |

## Usage Guidelines

You use the **shape average** policy-map class command to control output traffic. Shaping is not supported in input policy maps.

Traffic shaping limits the rate of transmission of data. Configuring traffic shaping for a user-defined class or **class-default** for class-based shaping sets the peak information rate (PIR) for that class. Configuring traffic shaping for the class **class-default** when it is the only class in the policy map that is attached to an interface sets the PIR for the interface (port shaping).

You cannot configure **shape average** in a class that includes priority queueing (configured with the **priority** policy-map class configuration command).

The **shape average** command uses a default queue limit for the class. You can change the queue limit by using the **queue-limit** policy-map class command, overriding the default that is set by the **shape average** command.

You cannot use the **bandwidth** policy-map class configuration command to configure class-based weighted fair queuing (CBWFQ) and the **shape average** command to configure traffic shaping for the same class.

You can configure hierarchical policy maps by attaching the **service-policy** policy-map class command to the class **class-default** only when **shape average** is also configured on the class **class-default**.

To return to policy-map configuration mode, use the **exit** command. To return to privileged EXEC mode, use the **end** command.

## Examples

This example shows how to configure traffic shaping for outgoing traffic on a Fast Ethernet port so that *outclass1*, *outclass2*, and *outclass3* get a maximum of 50, 20, and 10 Mbps of the buffer size. The class **class-default** gets the remaining bandwidth.

```
Switch(config)# policy-map out-policy
Switch(config-pmap)# class classout1
Switch(config-pmap-c)# shape average 50000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout2
Switch(config-pmap-c)# shape average 20000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# class classout3
Switch(config-pmap-c)# shape average 10000000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet 0/1
Switch(config-if)# service-policy out out-policy
```

This example shows how to configure port shaping by configuring a hierarchical policy map that shapes a port to 90 Mbps, allocated according to the *out-policy* policy map configured in the previous example.

```
Switch(config)# policy-map out-policy-parent
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# shape average 90000000
Switch(config-pmap-c)# service-policy out-policy
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

You can verify your settings by entering the **show policy-map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **show policy-map** | Displays QoS policy maps. |
| **show policy-map interface** [*interface-id*] | Displays policy maps configured on the specified interface or on all interfaces. |

# show access-lists

Use the **show access-lists** privileged EXEC command to display access control lists (ACLs) configured on the switch.

**show access-lists** [*name* | *number* | **hardware counters** | **ipc**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *name* | (Optional) Name of the ACL. |
| *number* | (Optional) ACL number. The range is 1 to 2699. |
| **hardware counters** | (Optional) Display global hardware ACL statistics for switched and routed packets. |
| **ipc** | (Optional) Display Interprocess Communication (IPC) protocol access-list configuration download information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **rate-limit** keywords are not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switch supports only IP standard and extended access lists. Therefore, the allowed numbers are only 1 to 199 and 1300 to 2699.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show access-lists** command:

```
Switch# show access-lists
Standard IP access list 1
    10 permit 1.1.1.1
    20 permit 2.2.2.2
    30 permit any
    40 permit 0.255.255.255, wildcard bits 12.0.0.0
Standard IP access list videowizard_1-1-1-1
    10 permit 1.1.1.1
Standard IP access list videowizard_10-10-10-10
    10 permit 10.10.10.10
Extended IP access list 121
    10 permit ahp host 10.10.10.10 host 20.20.10.10 precedence routine
```

This is an example of output from the **show access-lists hardware counters** command:

```
Switch# show access-lists hardware counters
L2 ACL INPUT Statistics
     Drop:                All frame count: 855
     Drop:                All bytes count: 94143
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 2121
     Forwarded:           All bytes count: 180762
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L3 ACL INPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 13586
     Forwarded:           All bytes count: 1236182
     Forwarded And Log:   All frame count: 0
     Forwarded And Log:   All bytes count: 0

 L2 ACL OUTPUT Statistics
     Drop:                All frame count: 0
     Drop:                All bytes count: 0
     Drop And Log:        All frame count: 0
     Drop And Log:        All bytes count: 0
     Bridge Only:         All frame count: 0
     Bridge Only:         All bytes count: 0
     Bridge Only And Log: All frame count: 0
     Bridge Only And Log: All bytes count: 0
     Forwarding To CPU:   All frame count: 0
     Forwarding To CPU:   All bytes count: 0
     Forwarded:           All frame count: 232983
     Forwarded:           All bytes count: 16825661
```

```
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0

L3 ACL OUTPUT Statistics
    Drop:                All frame count: 0
    Drop:                All bytes count: 0
    Drop And Log:        All frame count: 0
    Drop And Log:        All bytes count: 0
    Bridge Only:         All frame count: 0
    Bridge Only:         All bytes count: 0
    Bridge Only And Log: All frame count: 0
    Bridge Only And Log: All bytes count: 0
    Forwarding To CPU:   All frame count: 0
    Forwarding To CPU:   All bytes count: 0
    Forwarded:           All frame count: 514434
    Forwarded:           All bytes count: 39048748
    Forwarded And Log:   All frame count: 0
    Forwarded And Log:   All bytes count: 0
```

## Related Commands

| Command | Description |
|---|---|
| **access-list** | Configures a standard or extended numbered access list on the switch. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.** |
| **ip access list** | Configures a named IP access list on the switch. For syntax information, select **Cisco IOS IP Command Reference, Volume 1 of 3:Addressing and Services, Release 12.2 > IP Services Commands.** |
| **mac access-list extended** | Configures a named or numbered MAC access list on the switch. |

# show archive status

Use the **show archive status** privileged EXEC command to display the status of a new image being downloaded to a switch with the HTTP or the TFTP protocol.

**show archive status** [ **|**{**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you use the **archive download-sw** privileged EXEC command to download an image to a TFTP server, the output of the **archive download-sw** command shows the status of the download.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

These are examples of output from the **show archive status** command:

```
Switch# show archive status
IDLE: No upgrade in progress

Switch# show archive status
LOADING: Upgrade in progress

Switch# show archive status
EXTRACT: Extracting the image

Switch# show archive status
VERIFY: Verifying software

Switch# show archive status
RELOAD: Upgrade completed. Reload pending
```

## Related Commands

| Command | Description |
|---|---|
| **archive download-sw** | Downloads a new image from a TFTP server to the switch. |

# show boot

Use the **show boot** privileged EXEC command to display the settings of the boot environment variables.

**show boot** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show boot** command. Table 2-4 describes each field in the display.

```
Switch# show boot
5d05h: %SYS-5-CONFIG_I: Configured from console by console
BOOT path-list      :
Config file         : flash:/config.text
Private Config file : flash:/private-config.text
Enable Break        : no
Manual Boot         : yes
HELPER path-list    :
Auto upgrade        : yes
```

*Table 2-4 show boot Field Descriptions*

| Field | Description |
|---|---|
| BOOT path-list | Displays a semicolon separated list of executable files to try to load and execute when automatically booting.<br>If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.<br>If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system. |
| Config file | Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. |

*Table 2-4 show boot Field Descriptions (continued)*

| Field | Description |
|---|---|
| Private Config file | Displays the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. |
| Enable Break | Displays whether a break during booting is enabled or disabled. If it is set to yes, on, or 1, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system is initialized. |
| Manual Boot | Displays whether the switch automatically or manually boots. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode. |
| Helper path-list | Displays a semicolon separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader. |

**Related Commands**

| Command | Description |
|---|---|
| **boot config-file** | Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration. |
| **boot enable-break** | Enables interrupting the automatic boot process. |
| **boot manual** | Enables manually booting the switch during the next boot cycle. |
| **boot private-config-file** | Specifies the filename that Cisco IOS uses to read and write a nonvolatile copy of the private configuration. |
| **boot system** | Specifies the Cisco IOS image to load during the next boot cycle. |

# show cable-diagnostics tdr

Use the **show cable-diagnostics tdr** privileged EXEC command to display the Time Domain Reflector (TDR) results.

**show cable-diagnostics tdr interface** *interface-id* [ | {**begin** | **exclude** | **include**} *expression*]

**Note** TDR is supported only on the copper Ethernet 10/100 ports on the Cisco ME switch.

## Syntax Description

| | |
|---|---|
| *interface-id* | Specify the interface on which TDR was run. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

TDR is supported only on copper Ethernet 10/100 ports on the Cisco ME switch. It is not supported on small form-factor pluggable (SFP)-module ports. For more information about TDR, see the software configuration guide for this release.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command on a Cisco ME switch:

```
Switch# show cable-diagnostics tdr interface fastethernet0/1
TDR test last run on: March 01 18:14:44

Interface Speed Local pair Pair length        Remote pair Pair status
--------- ----- ---------- ------------------ ----------- --------------------
Fa0/1     100M  Pair A     4    +/- 5  meters Pair A      Normal
                Pair B     4    +/- 5  meters Pair B      Normal
                Pair C     N/A                Pair C      N/A
                Pair D     N/A                Pair D      N/A
```

Table 2-5 lists the descriptions of the fields in the **show cable-diagnostics tdr** command output.

*Table 2-5 Fields Descriptions for the show cable-diagnostics tdr Command Output*

| Field | Description |
|---|---|
| Interface | Interface on which TDR was run. |
| Speed | Speed of connection. |
| Local pair | Name of the pair of wires that TDR is testing on the local interface. |
| Pair length | Location on the cable where the problem is, with respect to your switch. TDR can only find the location in one of these cases:<br>• The cable is properly connected, the link is up, and the interface speed is 100 Mbps.<br>• The cable is open.<br>• The cable has a short. |
| Remote pair | Name of the pair of wires to which the local pair is connected. TDR can learn about the remote pair only when the cable is properly connected and the link is up. |
| Pair status | The status of the pair of wires on which TDR is running:<br>• Normal—The pair of wires is properly connected.<br>• Not completed—The test is running and is not completed.<br>• Not supported—The interface does not support TDR.<br>• Open—The pair of wires is open.<br>• Shorted—The pair of wires is shorted. |

This is an example of output from the **show interface** *interface-id* command when TDR is running:

```
Switch# show interface fastethernet0/1
fastethernet0/1 is up, line protocol is up (connected: TDR in Progress)
```

This is an example of output from the **show cable-diagnostics tdr interface** *interface-id* command when TDR is not running:

```
Switch# show cable-diagnostics tdr interface fastethernet0/1
% TDR test was never issued on fa0/1
```

If an interface does not support TDR, this message appears:

```
% TDR test is not supported on switch 1
```

## Related Commands

| Command | Description |
|---|---|
| test cable-diagnostics tdr | Enables and runs TDR on an interface. |

# show class-map

Use the **show class-map** user EXEC command to display quality of service (QoS) class maps, which define the match criteria to classify traffic.

**show class-map** [*class-map-name*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *class-map-name* | (Optional) Display the contents of the specified class map. |
| **| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show class-map** command:

```
Switch> show class-map
Class Map match-all videowizard_10-10-10-10 (id 2)
   Match access-group name videowizard_10-10-10-10

 Class Map match-any class-default (id 0)
   Match any
 Class Map match-all dscp5 (id 3)
   Match ip dscp 5
```

## Related Commands

| Command | Description |
|---|---|
| **class-map** | Creates a class map to be used for matching packets to the class whose name you specify. |
| **match access-group** | Defines the match criteria to classify traffic. |

# show controllers cpu-interface

Use the **show controllers cpu-interface** privileged EXEC command to display the state of the CPU network interface ASIC and the send and receive statistics for packets reaching the CPU.

**show controllers cpu-interface** [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is a partial output example from the **show controllers cpu-interface** command:

```
Switch# show controllers cpu-interface
cpu-queue-frames  retrieved  dropped    invalid    hol-block
----------------- ---------- ---------- ---------- ----------
rpc               4523063    0          0          0
stp               1545035    0          0          0
ipc               1903047    0          0          0
routing protocol  96145      0          0          0
L2 protocol       79596      0          0          0
remote console    0          0          0          0
sw forwarding     5756       0          0          0
host              225646     0          0          0
broadcast         46472      0          0          0
cbt-to-spt        0          0          0          0
igmp snooping     68411      0          0          0
icmp              0          0          0          0
logging           0          0          0          0
rpf-fail          0          0          0          0
queue14           0          0          0          0
cpu heartbeat     1710501    0          0          0
```

```
Supervisor ASIC receive-queue parameters
----------------------------------------
 queue 0 maxrecevsize 5EE pakhead 1419A20 paktail 13EAED4
 queue 1 maxrecevsize 5EE pakhead 15828E0 paktail 157FBFC
 queue 2 maxrecevsize 5EE pakhead 1470D40 paktail 1470FE4
 queue 3 maxrecevsize 5EE pakhead 19CDDD0 paktail 19D02C8

<output truncated>

Supervisor ASIC Mic Registers
-----------------------------
MicDirectPollInfo               80000800
MicIndicationsReceived          00000000
MicInterruptsReceived           00000000
MicPcsInfo                      0001001F
MicPlbMasterConfiguration       00000000
MicRxFifosAvailable             00000000
MicRxFifosReady                 0000BFFF
MicTimeOutPeriod:       FrameTOPeriod: 00000EA6 DirectTOPeriod: 00004000

<output truncated>

MicTransmitFifoInfo:
Fifo0:   StartPtrs:     038C2800        ReadPtr:        038C2C38
        WritePtrs:      038C2C38        Fifo_Flag:      8A800800
        Weights:        001E001E
Fifo1:  StartPtr:       03A9BC00        ReadPtr:        03A9BC60
        WritePtrs:      03A9BC60        Fifo_Flag:      89800400
        writeHeaderPtr: 03A9BC60
Fifo2:  StartPtr:       038C8800        ReadPtr:        038C88E0
        WritePtrs:      038C88E0        Fifo_Flag:      88800200
        writeHeaderPtr: 038C88E0
Fifo3:  StartPtr:       03C30400        ReadPtr:        03C30638
        WritePtrs:      03C30638        Fifo_Flag:      89800400
        writeHeaderPtr: 03C30638
Fifo4:  StartPtr:       03AD5000        ReadPtr:        03AD50A0
        WritePtrs:      03AD50A0        Fifo_Flag:      89800400
        writeHeaderPtr: 03AD50A0
Fifo5:  StartPtr:       03A7A600        ReadPtr:        03A7A600
        WritePtrs:      03A7A600        Fifo_Flag:      88800200
        writeHeaderPtr: 03A7A600
Fifo6:  StartPtr:       03BF8400        ReadPtr:        03BF87F0
        WritePtrs:      03BF87F0        Fifo_Flag:      89800400

<output truncated>
```

## Related Commands

| Command | Description |
|---|---|
| **show controllers ethernet-controller** | Displays per-interface send and receive statistics read from the hardware or the interface internal registers. |
| **show interfaces** | Displays the administrative and operational status of all interfaces or a specified interface. |

# show controllers ethernet-controller

Use the **show controllers ethernet-controller** privileged EXEC command without keywords to display per-interface send and receive statistics read from the hardware. Use with the **phy** keyword to display the interface internal registers or the **port-asic** keyword to display information about the port ASIC.

**show controllers ethernet-controller** [*interface-id*] [**phy** [**detail**]] [**port-asic** {**configuration** | **statistics**}] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | The physical interface (including type, module, and port number). |
| **phy** | (Optional) Display the status of the internal registers on the switch physical layer device (PHY) for the device or the interface. This display includes the operational state of the automatic medium-dependent interface crossover (Auto-MDIX) feature on an interface. |
| **detail** | (Optional) Display details about the PHY internal registers. |
| **port-asic** | (Optional) Display information about the port ASIC internal registers. |
| **configuration** | Display port ASIC internal register configuration. |
| **statistics** | Display port ASIC statistics, including the Rx/Sup Queue and miscellaneous statistics. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC (only supported with the *interface-id* keywords in user EXEC mode)

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This display without keywords provides traffic statistics, basically the RMON statistics for all interfaces or for the specified interface.

When you enter the **phy** or **port-asic** keywords, the displayed information is useful primarily for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show controllers ethernet-controller** command for an interface. Table 2-6 describes the *Transmit* fields, and Table 2-7 describes the *Receive* fields.

```
Switch# show controllers ethernet-controller gigabitethernet0/1
Transmit GigabitEthernet0/1            Receive
         0 Bytes                               0 Bytes
         0 Unicast frames                      0 Unicast frames
         0 Multicast frames                    0 Multicast frames
         0 Broadcast frames                    0 Broadcast frames
         0 Too old frames                      0 Unicast bytes
         0 Deferred frames                     0 Multicast bytes
         0 MTU exceeded frames                 0 Broadcast bytes
         0 1 collision frames                  0 Alignment errors
         0 2 collision frames                  0 FCS errors
         0 3 collision frames                  0 Oversize frames
         0 4 collision frames                  0 Undersize frames
         0 5 collision frames                  0 Collision fragments
         0 6 collision frames
         0 7 collision frames                  0 Minimum size frames
         0 8 collision frames                  0 65 to 127 byte frames
         0 9 collision frames                  0 128 to 255 byte frames
         0 10 collision frames                 0 256 to 511 byte frames
         0 11 collision frames                 0 512 to 1023 byte frames
         0 12 collision frames                 0 1024 to 1518 byte frames
         0 13 collision frames                 0 Overrun frames
         0 14 collision frames                 0 Pause frames
         0 15 collision frames                 0 Symbol error frames
         0 Excessive collisions
         0 Late collisions                     0 Invalid frames, too large
         0 VLAN discard frames                 0 Valid frames, too large
         0 Excess defer frames                 0 Invalid frames, too small
         0 64 byte frames                      0 Valid frames, too small
         0 127 byte frames
         0 255 byte frames                     0 Too old frames
         0 511 byte frames                     0 Valid oversize frames
         0 1023 byte frames                    0 System FCS error frames
         0 1518 byte frames                    0 RxPortFifoFull drop frame
         0 Too large frames
         0 Good (1 coll) frames
```

***Table 2-6 Transmit Field Descriptions***

| Field | Description |
|---|---|
| Bytes | The total number of bytes sent on an interface. |
| Unicast Frames | The total number of frames sent to unicast addresses. |
| Multicast frames | The total number of frames sent to multicast addresses. |
| Broadcast frames | The total number of frames sent to broadcast addresses. |
| Too old frames | The number of frames dropped on the egress port because the packet aged out. |
| Deferred frames | The number of frames that are not sent after the time exceeds 2*maximum-packet time. |
| MTU exceeded frames | The number of frames that are larger than the maximum allowed frame size. |
| 1 collision frames | The number of frames that are successfully sent on an interface after one collision occurs. |
| 2 collision frames | The number of frames that are successfully sent on an interface after two collisions occur. |
| 3 collision frames | The number of frames that are successfully sent on an interface after three collisions occur. |
| 4 collision frames | The number of frames that are successfully sent on an interface after four collisions occur. |

*Table 2-6 Transmit Field Descriptions (continued)*

| Field | Description |
|---|---|
| 5 collision frames | The number of frames that are successfully sent on an interface after five collisions occur. |
| 6 collision frames | The number of frames that are successfully sent on an interface after six collisions occur. |
| 7 collision frames | The number of frames that are successfully sent on an interface after seven collisions occur. |
| 8 collision frames | The number of frames that are successfully sent on an interface after eight collisions occur. |
| 9 collision frames | The number of frames that are successfully sent on an interface after nine collisions occur. |
| 10 collision frames | The number of frames that are successfully sent on an interface after ten collisions occur. |
| 11 collision frames | The number of frames that are successfully sent on an interface after 11 collisions occur. |
| 12 collision frames | The number of frames that are successfully sent on an interface after 12 collisions occur. |
| 13 collision frames | The number of frames that are successfully sent on an interface after 13 collisions occur. |
| 14 collision frames | The number of frames that are successfully sent on an interface after 14 collisions occur. |
| 15 collision frames | The number of frames that are successfully sent on an interface after 15 collisions occur. |
| Excessive collisions | The number of frames that could not be sent on an interface after 16 collisions occur. |
| Late collisions | After a frame is sent, the number of frames dropped because late collisions were detected while the frame was sent. |
| VLAN discard frames | The number of frames dropped on an interface because the CFI[1] bit is set. |
| Excess defer frames | The number of frames that are not sent after the time exceeds the maximum-packet time. |
| 64 byte frames | The total number of frames sent on an interface that are 64 bytes. |
| 127 byte frames | The total number of frames sent on an interface that are from 65 to 127 bytes. |
| 255 byte frames | The total number of frames sent on an interface that are from 128 to 255 bytes. |
| 511 byte frames | The total number of frames sent on an interface that are from 256 to 511 bytes. |
| 1023 byte frames | The total number of frames sent on an interface that are from 512 to 1023 bytes. |
| 1518 byte frames | The total number of frames sent on an interface that are from 1024 to 1518 bytes. |
| Too large frames | The number of frames sent on an interface that are larger than the maximum allowed frame size. |
| Good (1 coll) frames | The number of frames that are successfully sent on an interface after one collision occurs. This value does not include the number of frames that are not successfully sent after one collision occurs. |

1. CFI = Canonical Format Indicator

*Table 2-7 Receive Field Descriptions*

| Field | Description |
|---|---|
| Bytes | The total amount of memory (in bytes) used by frames received on an interface, including the FCS[1] value and the incorrectly formed frames. This value excludes the frame header bits. |
| Unicast frames | The total number of frames successfully received on the interface that are directed to unicast addresses. |
| Multicast frames | The total number of frames successfully received on the interface that are directed to multicast addresses. |
| Broadcast frames | The total number of frames successfully received on an interface that are directed to broadcast addresses. |

*Table 2-7 Receive Field Descriptions (continued)*

| Field | Description |
|---|---|
| Unicast bytes | The total amount of memory (in bytes) used by unicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits. |
| Multicast bytes | The total amount of memory (in bytes) used by multicast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits. |
| Broadcast bytes | The total amount of memory (in bytes) used by broadcast frames received on an interface, including the FCS value and the incorrectly formed frames. This value excludes the frame header bits. |
| Alignment errors | The total number of frames received on an interface that have alignment errors. |
| FCS errors | The total number of frames received on an interface that have a valid length (in bytes) but do not have the correct FCS values. |
| Oversize frames | The number of frames received on an interface that are larger than the maximum allowed frame size. |
| Undersize frames | The number of frames received on an interface that are smaller than 64 bytes. |
| Collision fragments | The number of collision fragments received on an interface. |
| Minimum size frames | The total number of frames that are the minimum frame size. |
| 65 to 127 byte frames | The total number of frames that are from 65 to 127 bytes. |
| 128 to 255 byte frames | The total number of frames that are from 128 to 255 bytes. |
| 256 to 511 byte frames | The total number of frames that are from 256 to 511 bytes. |
| 512 to 1023 byte frames | The total number of frames that are from 512 to 1023 bytes. |
| 1024 to 1518 byte frames | The total number of frames that are from 1024 to 1518 bytes. |
| Overrun frames | The total number of overrun frames received on an interface. |
| Pause frames | The number of pause frames received on an interface. |
| Symbol error frames | The number of frames received on an interface that have symbol errors. |
| Invalid frames, too large | The number of frames received that were larger than maximum allowed MTU[2] size (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error. |
| Valid frames, too large | The number of frames received on an interface that are larger than the maximum allowed frame size. |
| Invalid frames, too small | The number of frames received that are smaller than 64 bytes (including the FCS bits and excluding the frame header) and that have either an FCS error or an alignment error. |
| Valid frames, too small | The number of frames received on an interface that are smaller than 64 bytes (or 68 bytes for VLAN-tagged frames) and that have valid FCS values. The frame size includes the FCS bits but excludes the frame header bits. |
| Too old frames | The number of frames dropped on the ingress port because the packet aged out. |
| Valid oversize frames | The number of frames received on an interface that are larger than the maximum allowed frame size and have valid FCS values. The frame size includes the FCS value but does not include the VLAN tag. |

*Table 2-7 Receive Field Descriptions (continued)*

| Field | Description |
|---|---|
| System FCS error frames | The total number of frames received on an interface that have a valid length (in bytes) but that do not have the correct FCS values. |
| RxPortFifoFull drop frames | The total number of frames received on an interface that are dropped because the ingress queue is full. |

1. FCS = frame check sequence
2. MTU = maximum transmission unit

This is an example of output from the **show controllers ethernet-controller phy** command for a specific interface. Note that the last line of the display is the setting for Auto-MDIX for the interface.

```
Switch# show controllers ethernet-controller gigabitethernet0/2 phy
Control Register                        :  0001 0001 0100 0000
 Control STATUS                          :  0111 1001 0100 1001
 Phy ID 1                                :  0000 0001 0100 0001
 Phy ID 2                                :  0000 1100 0010 0100
 Auto-Negotiation Advertisement          :  0000 0011 1110 0001
 Auto-Negotiation Link Partner           :  0000 0000 0000 0000
 Auto-Negotiation Expansion Reg          :  0000 0000 0000 0100
 Next Page Transmit Register             :  0010 0000 0000 0001
 Link Partner Next page Registe          :  0000 0000 0000 0000
 1000BASE-T Control Register             :  0000 1111 0000 0000
 1000BASE-T Status Register              :  0100 0000 0000 0000
 Extended Status Register                :  0011 0000 0000 0000
 PHY Specific Control Register           :  0000 0000 0111 1000
 PHY Specific Status Register            :  1000 0001 0100 0000
 Interrupt Enable                        :  0000 0000 0000 0000
 Interrupt Status                        :  0000 0000 0100 0000
 Extended PHY Specific Control           :  0000 1100 0110 1000
 Receive Error Counter                   :  0000 0000 0000 0000
 Reserved Register 1                     :  0000 0000 0000 0000
 Global Status                           :  0000 0000 0000 0000
 LED Control                             :  0100 0001 0000 0000
 Manual LED Override                     :  0000 1000 0010 1010
 Extended PHY Specific Control           :  0000 0000 0001 1010
 Disable Receiver 1                      :  0000 0000 0000 1011
 Disable Receiver 2                      :  1000 0000 0000 0100
 Extended PHY Specific Status            :  1000 0100 1000 0000
 Auto-MDIX                               :  On   [AdminState=1   Flags=0x00052248]
```

This is an example of output from the **show controllers ethernet-controller port-asic configuration** command:

```
Switch# show controllers ethernet-controller port-asic configuration
================================================================================
PortASIC 0 Registers
--------------------------------------------------------------------------------
DeviceType                          : 000101BC
Reset                               : 00000000
PmadMicConfig                       : 00000001
PmadMicDiag                         : 00000003
SupervisorReceiveFifoSramInfo       : 000007D0 000007D0 40000000
SupervisorTransmitFifoSramInfo      : 000001D0 000001D0 40000000
GlobalStatus                        : 00000800
IndicationStatus                    : 00000000
IndicationStatusMask                : FFFFFFFF
InterruptStatus                     : 00000000
InterruptStatusMask                 : 01FFE800
```

```
SupervisorDiag                     : 00000000
SupervisorFrameSizeLimit           : 000007C8
SupervisorBroadcast                : 000A0F01
GeneralIO                          : 000003F9 00000000 00000004
StackPcsInfo                       : FFFF1000 860329BD 5555FFFF FFFFFFFF
                                     FF0FFF00 86020000 5555FFFF 00000000
StackRacInfo                       : 73001630 00000003 7F001644 00000003
                                     24140003 FD632B00 18E418E0 FFFFFFFF
StackControlStatus                 : 18E418E0
stackControlStatusMask             : FFFFFFFF
TransmitBufferFreeListInfo         : 00000854 00000800 00000FF8 00000000
                                     0000088A 0000085D 00000FF8 00000000
TransmitRingFifoInfo               : 00000016 00000016 40000000 00000000
                                     0000000C 0000000C 40000000 00000000
TransmitBufferInfo                 : 00012000 00000FFF 00000000 00000030
TransmitBufferCommonCount          : 00000F7A
TransmitBufferCommonCountPeak      : 0000001E
TransmitBufferCommonCommonEmpty    : 000000FF
NetworkActivity                    : 00000000 00000000 00000000 02400000
DroppedStatistics                  : 00000000
FrameLengthDeltaSelect             : 00000001
SneakPortFifoInfo                  : 00000000
MacInfo                            : 0EC0801C 00000001 0EC0801B 00000001
                                     00C0001D 00000001 00C0001E 00000001

<output truncated>
```

This is an example of output from the **show controllers ethernet-controller port-asic statistics** command:

```
Switch# show controllers ethernet-controller port-asic statistics
==========================================================================
 PortASIC 0 Statistics
--------------------------------------------------------------------------
         0 RxQ-0, wt-0 enqueue frames           0 RxQ-0, wt-0 drop frames
   4118966 RxQ-0, wt-1 enqueue frames           0 RxQ-0, wt-1 drop frames
         0 RxQ-0, wt-2 enqueue frames           0 RxQ-0, wt-2 drop frames

         0 RxQ-1, wt-0 enqueue frames           0 RxQ-1, wt-0 drop frames
       296 RxQ-1, wt-1 enqueue frames           0 RxQ-1, wt-1 drop frames
   2836036 RxQ-1, wt-2 enqueue frames           0 RxQ-1, wt-2 drop frames

         0 RxQ-2, wt-0 enqueue frames           0 RxQ-2, wt-0 drop frames
         0 RxQ-2, wt-1 enqueue frames           0 RxQ-2, wt-1 drop frames
    158377 RxQ-2, wt-2 enqueue frames           0 RxQ-2, wt-2 drop frames

         0 RxQ-3, wt-0 enqueue frames           0 RxQ-3, wt-0 drop frames
         0 RxQ-3, wt-1 enqueue frames           0 RxQ-3, wt-1 drop frames
         0 RxQ-3, wt-2 enqueue frames           0 RxQ-3, wt-2 drop frames


        15 TxBufferFull Drop Count              0 Rx Fcs Error Frames
         0 TxBufferFrameDesc BadCrc16           0 Rx Invalid Oversize Frames
         0 TxBuffer Bandwidth Drop Cou          0 Rx Invalid Too Large Frames
         0 TxQueue Bandwidth Drop Coun          0 Rx Invalid Too Large Frames
         0 TxQueue Missed Drop Statist          0 Rx Invalid Too Small Frames
        74 RxBuffer Drop DestIndex Cou          0 Rx Too Old Frames
         0 SneakQueue Drop Count                0 Tx Too Old Frames
         0 Learning Queue Overflow Fra          0 System Fcs Error Frames
         0 Learning Cam Skip Count

        15 Sup Queue 0 Drop Frames              0 Sup Queue 8 Drop Frames
         0 Sup Queue 1 Drop Frames              0 Sup Queue 9 Drop Frames
         0 Sup Queue 2 Drop Frames              0 Sup Queue 10 Drop Frames
```

```
          0 Sup Queue 3 Drop Frames                0 Sup Queue 11 Drop Frames
          0 Sup Queue 4 Drop Frames                0 Sup Queue 12 Drop Frames
          0 Sup Queue 5 Drop Frames                0 Sup Queue 13 Drop Frames
          0 Sup Queue 6 Drop Frames                0 Sup Queue 14 Drop Frames
          0 Sup Queue 7 Drop Frames                0 Sup Queue 15 Drop Frames
================================================================================
 PortASIC 1 Statistics
--------------------------------------------------------------------------------
          0 RxQ-0, wt-0 enqueue frames             0 RxQ-0, wt-0 drop frames
         52 RxQ-0, wt-1 enqueue frames             0 RxQ-0, wt-1 drop frames
          0 RxQ-0, wt-2 enqueue frames             0 RxQ-0, wt-2 drop frames

<output truncated>
```

## Related Commands

| Command | Description |
|---|---|
| **show controllers cpu-interface** | Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU. |
| **show controllers tcam** | Displays the state of registers for all ternary content addressable memory (TCAM) in the system and for TCAM interface ASICs that are CAM controllers. |

# show controllers tcam

Use the **show controllers tcam** privileged EXEC command to display the state of the registers for all ternary content addressable memory (TCAM) in the system and for all TCAM interface ASICs that are CAM controllers.

**show controllers tcam** [**asic** [**number**]] [**detail**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **asic** | (Optional) Display port ASIC TCAM information. |
| **number** | (Optional) Display information for the specified port ASIC number. The range is from 0 to 15. |
| **detail** | (Optional) Display detailed TCAM register information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This display provides information that might be useful for Cisco technical support representatives troubleshooting the switch.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show controllers tcam** command:

```
Switch# show controllers tcam
------------------------------------------------------------------------
TCAM-0 Registers
------------------------------------------------------------------------
  REV:    00B30103
  SIZE:   00080040
  ID:     00000000
  CCR:    00000000_F0000020

  RPID0:  00000000_00000000
  RPID1:  00000000_00000000
  RPID2:  00000000_00000000
  RPID3:  00000000_00000000
```

```
  HRR0:   00000000_E000CAFC
  HRR1:   00000000_00000000
  HRR2:   00000000_00000000
  HRR3:   00000000_00000000
  HRR4:   00000000_00000000
  HRR5:   00000000_00000000
  HRR6:   00000000_00000000
  HRR7:   00000000_00000000
<output truncated>

  GMR31:  FF_FFFFFFFF_FFFFFFFF
  GMR32:  FF_FFFFFFFF_FFFFFFFF
  GMR33:  FF_FFFFFFFF_FFFFFFFF

================================================================================
 TCAM related PortASIC 1 registers
================================================================================
LookupType:                   89A1C67D_24E35F00
LastCamIndex:                 0000FFE0
LocalNoMatch:                 000069E0
ForwardingRamBaseAddress:
                              00022A00 0002FE00 00040600 0002FE00 0000D400
                              00000000 003FBA00 00009000 00009000 00040600
                              00000000 00012800 00012900
```

## Related Commands

| Command | Description |
|---|---|
| **show controllers cpu-interface** | Displays the state of the CPU network ASIC and send and receive statistics for packets reaching the CPU. |
| **show controllers ethernet-controller** | Displays per-interface send and receive statistics read from the hardware or the interface internal registers. |

# show controllers utilization

Use the **show controllers utilization** user EXEC command to display bandwidth utilization on the switch or specific ports.

**show controllers** [*interface-id*] **utilization** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) ID of the switch interface. |
| **\| begin** | (Optional) Display begins with the line that matches the specified *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the specified *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show controllers utilization** command.

```
Switch> show controllers utilization
Port       Receive Utilization  Transmit Utilization
Fa0/1            0                    0
Fa0/2            0                    0
Fa0/3            0                    0
Fa0/4            0                    0
Fa0/5            0                    0
Fa0/6            0                    0
Fa0/7            0                    0

<output truncated>

Switch Receive Bandwidth Percentage Utilization  : 0
Switch Transmit Bandwidth Percentage Utilization : 0

Switch Fabric Percentage Utilization : 0
```

This is an example of output from the **show controllers utilization** command on a specific port:

```
Switch> show controllers gigabitethernet0/1 utilization
Receive Bandwidth Percentage Utilization   : 0
Transmit Bandwidth Percentage Utilization  : 0
```

*Table 2-8 show controllers utilization Field Descriptions*

| Field | Description |
|---|---|
| Receive Bandwidth Percentage Utilization | Displays the received bandwidth usage of the switch, which is the sum of the received traffic on all the ports divided by the switch receive capacity. |
| Transmit Bandwidth Percentage Utilization | Displays the transmitted bandwidth usage of the switch, which is the sum of the transmitted traffic on all the ports divided it by the switch transmit capacity. |
| Fabric Percentage Utilization | Displays the average of the transmitted and received bandwidth usage of the switch. |

## Related Commands

| Command | Description |
|---|---|
| **show controllers ethernet-controller** | Displays the interface internal registers. |

# show dot1x

Use the **show dot1x** privileged EXEC command to display IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port.

**show dot1x** [**all** | **interface** *interface-id* | **statistics interface** *interface-id*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display the IEEE 802.1x status for all ports. |
| **interface** *interface-id* | (Optional) Display the IEEE 802.1x status for the specified port (including type, module, and port number). |
| **statistics interface** *interface-id* | (Optional) Display IEEE 802.1x statistics for the specified port (including type, module, and port number). |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a port, global parameters and a summary appear. If you specify a port, details for that port appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show dot1x** and the **show dot1x all** privileged EXEC commands:

```
Switch# show dot1x
Sysauthcontrol                  = Enabled
Supplicant Allowed In Guest Vlan  = Disabled
Dot1x Protocol Version          = 1
Dot1x Oper Controlled Directions  = Both
Dot1x Admin Controlled Directions = Both

Switch# show dot1x all
Dot1x Info for interface GigabitEthernet0/1
--------------------------------------------------
```

```
Supplicant MAC 00d0.b71b.35de
   AuthSM State      = CONNECTING
   BendSM State      = IDLE
PortStatus        = UNAUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0

Dot1x Info for interface GigabitEthernet0/2
----------------------------------------------------
PortStatus        = UNAUTHORIZED
MaxReq            = 2
HostMode          = Multi
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

This is an example of output from the **show dot1x interface** *interface-id* privileged EXEC command:

```
Switch# show dot1x interface gigabitethernet0/1
Supplicant MAC 00d0.b71b.35de
   AuthSM State      = AUTHENTICATED
   BendSM State      = IDLE
PortStatus        = AUTHORIZED
MaxReq            = 2
HostMode          = Single
Port Control      = Auto
QuietPeriod       = 60 Seconds
Re-authentication = Disabled
ReAuthPeriod      = 3600 Seconds
ServerTimeout     = 30 Seconds
SuppTimeout       = 30 Seconds
TxPeriod          = 30 Seconds
Guest-Vlan        = 0
```

This is an example of output from the **show dot1x statistics interface** *interface-id* command. Table 2-9 describes the fields in the display.

```
Switch# show dot1x statistics interface gigabitethernet0/1
PortStatistics Parameters for Dot1x
---------------------------------------------
TxReqId = 15    TxReq = 0       TxTotal = 15
RxStart = 4     RxLogoff = 0    RxRespId = 1    RxResp = 1
RxInvalid = 0   RxLenErr = 0    RxTotal= 6
RxVersion = 1   LastRxSrcMac 00d0.b71b.35de
```

*Table 2-9 show dot1x statistics Field Descriptions*

| Field | Description |
|---|---|
| TxReqId | Number of Extensible Authentication Protocol (EAP)-request/identity frames that have been sent. |
| TxReq | Number of EAP-request frames (other than request/identity frames) that have been sent. |
| TxTotal | Number of Extensible Authentication Protocol over LAN (EAPOL) frames of any type that have been sent. |
| RxStart | Number of valid EAPOL-start frames that have been received. |
| RxLogoff | Number of EAPOL-logoff frames that have been received. |
| RxRespId | Number of EAP-response/identity frames that have been received. |
| RxResp | Number of valid EAP-response frames (other than response/identity frames) that have been received. |
| RxInvalid | Number of EAPOL frames that have been received and have an unrecognized frame type. |
| RxLenError | Number of EAPOL frames that have been received in which the packet body length field is invalid. |
| RxTotal | Number of valid EAPOL frames of any type that have been received. |
| RxVersion | Number of received packets in the IEEE 802.1x Version 1 format. |
| LastRxSrcMac | Source MAC address carried in the most recently received EAPOL frame. |

## Related Commands

| Command | Description |
|---|---|
| **dot1x default** | Resets the configurable IEEE 802.1x parameters to their default values. |

# show env

Use the **show env** user EXEC command to display fan, temperature, redundant power system (RPS) availability, and power information for the switch.

**show env** {**all** | **fan** | **power** | **rps** | **temperature [status]**} [ | {**begin** | **exclude** | **include**} *expression*]

**Note** Although visible in the command-line interface, the status keyword is not suppported.

## Syntax Description

| | |
|---|---|
| **all** | Display both fan and temperature environmental status. |
| **fan** | Display the switch fan status. |
| **power** | Display the switch power status. |
| **rps** | Display whether a Cisco RPS 300 Redundant Power System is connected to the switch. This keyword is not visible on all platforms; the Cisco ME switch does not support the RPS |
| **temperature** | Display the switch temperature status as OK or FAULTY. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show env all** command:

```
Switch# show env all
FAN is OK
TEMPERATURE is OK
POWER is OK
RPS is NOT PRESENT
```

This is an example of output from the **show env fan** command:

```
Switch> show env fan
FAN is OK
```

# show errdisable detect

Use the **show errdisable detect** user EXEC command to display error-disable detection status.

**show errdisable detect** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(37)SE | The `Mode` column was added to the output display. |

## Usage Guidelines

The `Mode` column shows the shutdown mode that was configured for the error-disabled reason:

- port—The physical port is error disabled if a violation occurs.
- vlan—The virtual port is disabled if a violation occurs.
- port/vlan—Some ports are configured for physical port disable, and others are configured for virtual port disable. Enter the **show running config** privileged EXEC command to see the configuration for each port.

A displayed `gbic-invalid` error in the `Reason` column refers to an invalid small form-factor pluggable (SFP) interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show errdisable detect** command:

```
Switch> show errdisable detect
ErrDisable Reason   Detection   Mode
-----------------   ---------   ----
arp-inspection      Enabled   port
bpduguard           Enabled   port
channel-misconfig   Enabled   port
community-limit     Enabled   port
dhcp-rate-limit     Enabled   port
dtp-flap            Enabled   port
gbic-invalid        Enabled   port
invalid-policy      Enabled   port
l2ptguard           Enabled   port
link-flap           Enabled   port
link-monitor-fail   Enabled   port
```

```
loopback            Enabled   port
lsgroup             Enabled   port
oam-remote-failur   Enabled   port
pagp-flap           Enabled   port
psecure-violation   Enabled   port/vlan
security-violatio   Enabled   port
sfp-config-mismat   Enabled   port
storm-control       Enabled   port
udld                Enabled   port
vmps                Enabled   port
```

**Note** Though visible in the output, the dtp-flap, l2ptguard, ilpower, storm-control, arp-inspection, and unicast-flood fields are not valid.

## Related Commands

| Command | Description |
|---|---|
| **errdisable detect cause** | Enables error-disable detection for a specific cause or all causes. |
| **show errdisable flap-values** | Displays error condition recognition information. |
| **show errdisable recovery** | Displays error-disable recovery timer information. |
| **show interfaces status** | Displays interface status or a list of interfaces in an error-disabled state. |

# show errdisable flap-values

Use the **show errdisable flap-values** user EXEC command to display conditions that cause an error to be recognized for a cause.

**show errdisable flap-values** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The *Flaps* column in the display shows how many changes to the state within the specified time interval will cause an error to be detected and a port to be disabled. For example, the display shows that an error will be assumed and the port shut down if three Dynamic Trunking Protocol (DTP)-state (port mode access/trunk) or Port Aggregation Protocol (PAgP) flap changes occur during a 30-second interval, or if 5 link-state (link up/down) changes occur during a 10-second interval.

```
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

**Note** Although visible in the output display, the switch does not support DTP.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show errdisable flap-values** command:

```
Switch> show errdisable flap-values
ErrDisable Reason    Flaps    Time (sec)
-----------------    ------   ----------
pagp-flap              3       30
dtp-flap               3       30
link-flap              5       10
```

## Related Commands

| Command | Description |
|---|---|
| **errdisable detect cause** | Enables error-disable detection for a specific cause or all causes. |
| **show errdisable detect** | Displays error-disable detection status. |
| **show errdisable recovery** | Displays error-disable recovery timer information. |
| **show interfaces status** | Displays interface status or a list of interfaces in error-disabled state. |

# show errdisable recovery

Use the **show errdisable recovery** user EXEC command to display the error-disable recovery timer information.

**show errdisable recovery** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

A *gbic-invalid error-disable* reason refers to an invalid small form-factor pluggable (SFP) module interface.

## Examples

This is an example of output from the **show errdisable recovery** command:

```
Switch> show errdisable recovery
ErrDisable Reason    Timer Status
-----------------    --------------
udld                 Disabled
bpduguard            Disabled
security-violatio    Disabled
channel-misconfig    Disabled
vmps                 Disabled
pagp-flap            Disabled
dtp-flap             Disabled
link-flap            Enabled
psecure-violation    Disabled
gbic-invalid         Disabled
dhcp-rate-limit      Disabled
unicast-flood        Disabled
storm-control        Disabled
arp-inspection       Disabled
loopback             Disabled

Timer interval:300 seconds

Interfaces that will be enabled at the next timeout:
```

```
Interface    Errdisable reason    Time left(sec)
---------    -----------------    --------------
Gi0/2        link-flap             279
```

**Note** Though visible in the output, the unicast-flood and DTP fields are not valid.

## Related Commands

| Command | Description |
|---|---|
| **errdisable recovery** | Configures the recover mechanism variables. |
| **show errdisable detect** | Displays error-disabled detection status. |
| **show errdisable flap-values** | Displays error condition recognition information. |
| **show interfaces status** | Displays interface status or a list of interfaces in error-disabled state. |

# show etherchannel

Use the **show etherchannel** user EXEC command to display EtherChannel information for a channel.

**show etherchannel** [*channel-group-number* {**detail** | **port** | **port-channel** | **protocol** | **summary**}] {**detail** | **load-balance** | **port** | **port-channel** | **protocol** | **summary**} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *channel-group*-number | (Optional) Number of the channel group. The range is 1 to 48. |
| **detail** | Display detailed EtherChannel information. |
| **load-balance** | Display the load-balance or frame-distribution scheme among ports in the port channel. |
| **port** | Display EtherChannel port information. |
| **port-channel** | Display port-channel information. |
| **protocol** | Display the protocol that is being used in the EtherChannel. |
| **summary** | Display a one-line summary per channel-group. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a *channel-group*, all channel groups are displayed.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show etherchannel 1 detail** command:

```
Switch> show etherchannel 1 detail
Group state = L2
Ports: 2   Maxports = 16
Port-channels: 1 Max Port-channels = 16
Protocol:   LACP
               Ports in the group:
               -------------------
Port: Gi0/1
------------

Port state    = Up Mstr In-Bndl
Channel group = 1           Mode = Active      Gcchange = -
Port-channel  = Po1         GC   =   -         Pseudo port-channel = Po1
Port index    = 0           Load = 0x00        Protocol =   LACP

Flags:  S - Device is sending Slow LACPDUs   F - Device is sending fast LACPDU
        A - Device is in active mode.        P - Device is in passive mode.

Local information:
                           LACP port     Admin     Oper    Port     Port
Port      Flags   State    Priority      Key       Key     Number   State
Gi0/1     SA      bndl     32768         0x0       0x1     0x0      0x3D

Age of the port in the current state: 01d:20h:06m:04s

               Port-channels in the group:
               ----------------------

Port-channel: Po1    (Primary Aggregator)
------------

Age of the Port-channel   = 01d:20h:20m:26s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:20m:20s    Gi0/2
```

This is an example of output from the **show etherchannel 1 summary** command:

```
Switch> show etherchannel 1 summary
Flags:  D - down        P - in port-channel
        I - stand-alone s - suspended
        H - Hot-standby (LACP only)
        R - Layer3      S - Layer2
        u - unsuitable for bundling
        U - in use      f - failed to allocate aggregator
        d - default port

Number of channel-groups in use: 1
Number of aggregators:           1
```

```
Group  Port-channel  Protocol    Ports
------+-------------+-----------+-----------------------------------------
1      Po1(SU)         LACP      Gi0/1(P)    Gi0/2(P)
```

This is an example of output from the **show etherchannel 1 port-channel** command:

```
Switch> show etherchannel 1 port-channel
                Port-channels in the group:
                ----------------------
Port-channel: Po1    (Primary Aggregator)

------------

Age of the Port-channel   = 01d:20h:24m:50s
Logical slot/port   = 10/1          Number of ports = 2
HotStandBy port = null
Port state          = Port-channel Ag-Inuse
Protocol            =   LACP

Ports in the Port-channel:

Index   Load   Port     EC state        No of bits
------+------+------+------------------+-----------
  0     00     Gi0/1    Active          0
  0     00     Gi0/2    Active          0

Time since last port bundled:    01d:20h:24m:44s    Gi0/2
```

This is an example of output from **show etherchannel protocol** command:

```
Switch# show etherchannel protocol
                Channel-group listing:
                ----------------------
Group: 1
----------
Protocol:  LACP

Group: 2
----------
Protocol:  PAgP
```

## Related Commands

| Command | Description |
|---|---|
| **channel-group** | Assigns an Ethernet port to an EtherChannel group. |
| **channel-protocol** | Restricts the protocol used on a port to manage channeling. |
| **interface port-channel** | Accesses or creates the port channel. |

# show flowcontrol

Use the **show flowcontrol** user EXEC command to display the flow control status and statistics.

**show flowcontrol** [**interface** *interface-id* | **module** *number*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Display the flow control status and statistics for a specific interface. |
| **module** *number* | (Optional) Display the flow control status and statistics for all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to display the flow control status and statistics on the switch or for a specific interface.

Use the **show flowcontrol** command to display information about all the switch interfaces. The output from the **show flowcontrol** command is the same as the output from the **show flowcontrol module** *number* command.

Use the **show flowcontrol interface** *interface-id* command to display information about a specific interface.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show flowcontrol** command.

```
Switch> show flowcontrol
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/1      Unsupp.  Unsupp.  off      off         0       0
Gi0/2      desired  off      off      off         0       0
Gi0/3      desired  off      off      off         0       0
<output truncated>
```

This is an example of output from the **show flowcontrol interface** *interface-id* command:

```
Switch> show flowcontrol interface gigabitethernet0/2
Port       Send FlowControl  Receive FlowControl  RxPause TxPause
           admin    oper     admin    oper
---------  -------- -------- -------- --------    ------- -------
Gi0/2      desired  off      off      off         0       0
```

## Related Commands

| Command | Description |
|---|---|
| **flowcontrol** | Sets the receive flow-control state for an interface. |

# show idprom

Use the **show idprom** user EXEC command to display the IDPROM information for a Gigabit Ethernet interface.

**show idprom** {**interface** *interface-id*} [**detail**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | Display the IDPROM information for the specified Gigabit Ethernet interface. |
| **detail** | (Optional) Display detailed IDPROM information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

This command applies only to Gigabit Ethernet interfaces and displays information about SFPs inserted in the SFP module slot.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show idprom interface** command for a Gigabit Ethernet interface:

Switch# **show idprom interface gigabitethernet0/1**

```
General SFP Information
---------------------------------------------
Identifier            :   0x03
Connector             :   0x07
Transceiver           :   0x00 0x00 0x00 0x00 0x00 0x00 0x00 0x00
Encoding              :   0x02
BR_Nominal            :   0x01
Vendor Name           :   CISCO-NEC
Vendor Part Number    :   OD-BP1511-23SL2
Vendor Revision       :   0x30 0x30 0x30 0x31
Vendor Serial Number  :   NEC08440067
---------------------------------------------
```

```
Other Information
-------------------------------------------------------
Port asic num         : 0
Port asic port num    : 0
XCVR init completed   : 1
Embedded PHY          : not present
SFP presence index    : 0
SFP iter cnt          : 697918

SFP failed oper flag  : 0x0
IIC error cnt         : 0
IIC error dsb cnt     : 0
IIC max sts cnt       : 4
Chk for link status   : 1
Link Status           : 1
Link Status Media     : 1
Preferred media       : 0
Resolved Media        : 1
Config Media          : 1
Access Count          : 0
Access Count Max      : 2
Port Rx Loss          : no
Port Tx Fault         : no
Port Tx Disable       : no

Sfp selection asic reg map
------------------------------
stbi                : 0x00
sfpControl          : 0x4C
Regs Loc            : 0xF0000000

-------------------------------------------------------

 Page 0 Registers
-------------------------------------------------------------------------
 0000: 1140 Control Register                    :  0001 0001 0100 0000
 0001: 6149 Control STATUS                      :  0110 0001 0100 1001
 0002: 0141 Phy ID 1                            :  0000 0001 0100 0001
 0003: 0C92 Phy ID 2                            :  0000 1100 1001 0010
 0004: 01E1 Auto-Negotiation Advertisement      :  0000 0001 1110 0001
 0005: 0000 Auto-Negotiation Link Partner       :  0000 0000 0000 0000
 0006: 0004 Auto-Negotiation Expansion Reg      :  0000 0000 0000 0100
 0007: 2001 Next Page Transmit Register         :  0010 0000 0000 0001
 0008: 0000 Link Partner Next page Registe      :  0000 0000 0000 0000
 0009: 0F00 1000BASE-T Control Register         :  0000 1111 0000 0000
 000A: 0000 1000BASE-T Status Register          :  0000 0000 0000 0000
 000F: 0000 Extended Status Register            :  0000 0000 0000 0000
 0010: 6028 PHY Specific Control Register       :  0110 0000 0010 1000
 0011: 6CC8 PHY Specific Status Register        :  0110 1100 1100 1000
 0012: 0000 Interrupt Enable Register           :  0000 0000 0000 0000
 0013: 0700 PHY Specific Status Register2       :  0000 0111 0000 0000
 0015: 01C0 Receive Error Counter               :  0000 0001 1100 0000

 0016: 0000 Page Address Register               :  0000 0000 0000 0000
 001A: 8040 PHY Specific Control Register2      :  1000 0000 0100 0000

<output truncated>
```

## Related Commands

| Command | Description |
|---|---|
| show controllers ethernet-controller | Displays per-interface send and receive statistics read from the hardware, interface internal registers, or port ASIC information. |

# show interfaces

Use the **show interfaces** privileged EXEC command to display the administrative and operational status of all interfaces or a specified interface.

**show interfaces** [*interface-id* | **vlan** *vlan-id*] [**accounting** | **capabilities** [**module** *number*] | **counters** | **description** | **etherchannel** | **flowcontrol** | **stats** | **status** [**err-disabled**] | **switchport** [ **module** *number*] | **transceiver** [**properties** | **detail**] [**module** *number*] | **trunk**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 48. |
| **vlan** *vlan-id* | (Optional) VLAN identification. The range is 1 to 4094. |
| **accounting** | (Optional) Display accounting information on the interface, including active protocols and input and output packets and octets. |
| **capabilities** | (Optional) Display the capabilities of all interfaces or the specified interface, including the features and options that you can configure on the interface. Though visible in the command line help, this option is not available for VLAN IDs. |
| **module** *number* | (Optional) Display **capabilities**, **switchport** configuration, or **transceiver** characteristics (depending on preceding keyword) of all interfaces on the switch. The only valid module number is 1. This option is not available if you have entered a specific interface ID. |
| **counters** | (Optional) See the **show interfaces counters** command. |
| **description** | (Optional) Display the administrative status and description set for an interface. |
| **etherchannel** | (Optional) Display interface EtherChannel information. |
| **flowcontrol** | (Optional) Display interface flowcontrol information |
| **stats** | (Optional) Display the input and output packets by switching path for the interface. |
| **status** | (Optional) Display the status of the interface. A status of *unsupported* in the Type field means that a non-Cisco small form-factor pluggable (SFP) module is inserted in the module slot. |
| **err-disabled** | (Optional) Display interfaces in error-disabled state. |
| **switchport** | (Optional) Display the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **transceiver** [**detail** \| **properties**] | (Optional) Display the physical properties of a CWDM[1] or DWDM[2] small form-factor (SFP) module interface. The keywords have these meanings:<br>• **detail—**(Optional) Display calibration properties, including high and low numbers and any alarm information.<br>• **properties—**(Optional) Display speed and duplex settings on an interface. |
| **trunk** | Display interface trunk information. If you do not specify an interface, only information for active trunking ports appears. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

1. coarse wavelength-division multiplexer
2. dense wavelength-division multiplexer

**Note** Though visible in the command-line help strings, the **backup**, **crb**, **fair-queue**, **irb**, **mac-accounting**, **precedence**, **private-vlan mapping**, **pruning random-detect**, **rate-limit**, and **shape** keywords are not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **show interfaces capabilities** command with different keywords has these results:

- Use the **show interface capabilities module 1** to display the capabilities of all interfaces on the switch. Entering any other number is invalid.
- Use the **show interfaces** *interface-id* **capabilities** to display the capabilities of the specified interface.
- Use the **show interfaces capabilities** (with no module number or interface ID) to display the capabilities of all interfaces on the switch.
- Use the **show interface switchport module 1** to display the switch port characteristics of all interfaces on the switch. Entering any other number is invalid.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show interfaces** command for an interface:

```
Switch# show interfaces gigabitethernet0/2
GigabitEthernet0/2 is down, line protocol is down
  Hardware is Gigabit Ethernet, address is 0009.43a7.d085 (bia 0009.43a7.d085)
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  input flow-control is off, output flow-control is off
  ARP type: ARPA, ARP Timeout 04:00:00 Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue :0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     2 packets input, 1040 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 watchdog, 0 multicast, 0 pause input
```

```
     0 input packets with dribble condition detected
     4 packets output, 1040 bytes, 0 underruns
     0 output errors, 0 collisions, 3 interface resets
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier, 0 PAUSE output
     0 output buffer failures, 0 output buffers swapped out
```

This is an example of output from the **show interfaces accounting** command.

```
Switch# show interfaces accounting
Vlan1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
                      IP    1094395  131900022     559555   84077157
           Spanning Tree     283896   17033760         42       2520
                     ARP      63738    3825680        231      13860
Interface Vlan2 is disabled
Vlan7
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
Vlan31
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

GigabitEthernet0/1
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.
GigabitEthernet0/2
                Protocol    Pkts In   Chars In   Pkts Out  Chars Out
No traffic sent or received on this interface.

<output truncated>
```

This is an example of output from the **show interfaces capabilities** command for an interface.

```
Switch# show interfaces gigabitethernet0/2 capabilities
GigabitEthernet0/2
  Model:                 ME-2400-24T-FA
  Type:                  10/100/1000BaseTX SFP
  Speed:                 10,100,1000,auto
  Duplex:                half,full,auto
  Trunk encap. type:     802.1Q
  Trunk mode:            on,off,desirable,nonegotiate
  Channel:               yes
  Broadcast suppression: percentage(0-100)
  Flowcontrol:           rx-(off,on,desired),tx-(none)
  Fast Start:            yes
  QoS scheduling:        rx-(not configurable on per port basis),tx-(4q2t)
  CoS rewrite:           yes
  ToS rewrite:           yes
  UDLD:                  yes
SPAN:                  source/destination
  PortSecure:            yes
  Dot1x:                 yes
```

This is an example of output from the **show interfaces** *interface* **description** command when the interface has been described as *Connects to Marketing* by using the **description** interface configuration command.

```
Switch# show interfaces gigabitethernet0/2 description
Interface Status         Protocol Description
Gi0/2       up             down     Connects to Marketing
```

This is an example of output from the **show interfaces etherchannel** command when port channels are configured on the switch:

```
Switch# show interfaces etherchannel
----
Port-channel1:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/1          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel2:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/2          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse

Port-channel3:
Age of the Port-channel   = 03d:20h:17m:29s
Logical slot/port   = 10/3          Number of ports = 0
GC                  = 0x00000000      HotStandBy port = null
Port state          = Port-channel Ag-Not-Inuse
```

This is an example of output from the **show interfaces stats** command for a specified VLAN interface.

```
Switch# show interfaces vlan 1 stats
Switching path    Pkts In   Chars In   Pkts Out  Chars Out
        Processor    1165354  136205310     570800   91731594
      Route cache          0          0          0          0
            Total    1165354  136205310     570800   91731594
```

This is an example of partial output from the **show interfaces status** command. It displays the status of all interfaces.

```
Switch# show interfaces status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/1                        connected    1          a-full  a-100 10/100BaseTX
Fa0/2                        connected    1          a-full  a-100 10/100BaseTX
Fa0/3                        notconnect   1            auto   auto 10/100BaseTX
Fa0/4                        disabled     1            auto   auto 10/100BaseTX
Fa0/5                        disabled     1            auto   auto 10/100BaseTX
Fa0/6                        disabled     1            auto   auto 10/100BaseTX
Fa0/7                        disabled     1            auto   auto 10/100BaseTX
Fa0/8                        disabled     1            auto   auto 10/100BaseTX
Fa0/9                        disabled     1            auto   auto 10/100BaseTX
Fa0/10                       disabled     1            auto   auto 10/100BaseTX
Fa0/11                       disabled     1            auto   auto 10/100BaseTX
Fa0/12                       disabled     1            auto   auto 10/100BaseTX
Fa0/13                       disabled     1            auto   auto 10/100BaseTX
Fa0/14                       disabled     1            auto   auto 10/100BaseTX
Fa0/15                       disabled     1            auto   auto 10/100BaseTX
Fa0/16                       disabled     1            auto   auto 10/100BaseTX
Fa0/17                       disabled     1            auto   auto 10/100BaseTX
Fa0/18                       disabled     1            auto   auto 10/100BaseTX
Fa0/19                       disabled     1            auto   auto 10/100BaseTX
Fa0/20                       disabled     1            auto   auto 10/100BaseTX
Fa0/21                       disabled     1            auto   auto 10/100BaseTX
Fa0/22                       disabled     1            auto   auto 10/100BaseTX
Fa0/23                       disabled     1            auto   auto 10/100BaseTX
Fa0/24                       disabled     1            auto   auto 10/100BaseTX
Gi0/1                        notconnect   1            auto   auto 10/100/1000Ba
seTX SFP
Gi0/2                        connected    vl-err-dis a-full a-1000 10/100/1000BaseTX
```

These are examples of output from the **show interfaces status** command for a specific interface when private VLANs are configured. Port 22 is configured as a private-VLAN host port. It is associated with primary VLAN 20 and secondary VLAN 25.

```
Switch# show interfaces fastethernet0/22 status
Port      Name               Status       Vlan       Duplex  Speed Type
Fa0/22                       connected    20,25      a-full  a-100 10/100BaseTX
```

In this example, port 2 is configured as a private-VLAN promiscuous port. The display shows only the primary VLAN 20.

```
Switch# show interfaces gigabitethernet0/2 status
Port      Name               Status       Vlan       Duplex  Speed Type
Gi0/2                        connected    20         a-full  a-100 10/100/1000BaseTX
```

This is an example of output from the **show interfaces status err-disabled** command for an interface:

```
Switch# show interfaces gigabitethernet0/2 status err-disabled

Port      Name               Status       Reason               Err-disabled Vlans
Gi0/2                        connected    elmi evc down        1,200
```

This is an example of output from the **show interfaces switchport** command for a single port. Table 2-10 describes the fields in the display.

**Note** Private VLAN trunks are not supported in this release, so those fields are not applicable.

```
Switch# show interfaces gigabitethernet0/1 switchport
Name: Gi0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none

Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
```

```
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Capture Mode Disabled
Capture VLANs Allowed: ALL

Unknown unicast blocked: disabled
Unknown multicast blocked: disabled
Appliance trust: none
```

*Table 2-10 show interfaces switchport Field Descriptions*

| Field | Description |
|---|---|
| Name | Displays the port name. |
| Switchport | Displays the administrative and operational status of the port. In this display, the port is in switchport mode. |
| Administrative Mode<br>Operational Mode | Displays the administrative and operational modes. |
| Administrative Trunking Encapsulation<br>Negotiation of Trunking | Displays the administrative and operational encapsulation method and whether trunking negotiation is enabled. |
| Access Mode VLAN | Displays the VLAN ID to which the port is configured. |
| Trunking Native Mode VLAN | Lists the VLAN ID of the trunk that is in native mode. |
| Administrative Native VLAN tagging | Displays whether or not VLAN tagging is enabled. |
| Administrative private-vlan host-association | Displays the administrative VLAN association for private-VLAN host ports. |
| Administrative private-vlan mapping | Displays the administrative VLAN mapping for private-VLAN promiscuous ports. |
| Operational private-vlan | Displays the operational private-VLAN status. |
| Trunking VLANs enabled | Lists the active VLANs on the trunk. |
| Capture VLANs allowed | Lists the allowed VLANs on the trunk. |
| Unknown unicast blocked<br>Unknown multicast blocked | Displays whether or not unknown multicast and unknown unicast traffic is blocked on the interface. |

This is an example of output from the **show interfaces switchport** command for a port configured as a private VLAN promiscuous port. The primary VLAN 20 is mapped to secondary VLANs 25, 30 and 35:

```
Switch# show interface gigabitethernet0/2 switchport
Name: Gi1/0/2
Switchport: Enabled
Administrative Mode: private-vlan promiscuous
Operational Mode: private-vlan promiscuous
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Administrative private-vlan host-association: none
Administrative private-vlan mapping: 20 (VLAN0020) 25 (VLAN0025) 30 (VLAN0030) 35
(VLAN0035)
Administrative private-vlan trunk native VLAN: none
```

```
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan:
20 (VLAN0020) 25 (VLAN0025)
30 (VLAN0030)
35 (VLAN0035)

<output truncated>
```

This is an example of output from the **show interfaces** *interface-id* **trunk** command. It displays trunking information for the port.

```
Switch# show interfaces gigabitethernet0/1 trunk
Port          Mode         Encapsulation  Status        Native vlan
Gi0/1         auto         negotiate      trunking      1

Port          Vlans allowed on trunk
Gi0/1         1-4094

Port          Vlans allowed and active in management domain
Gi0/1         1-4

Port          Vlans in spanning tree forwarding state and not pruned
Gi0/1         1-4
```

This is an example of output from the **show interfaces transceiver properties** command. If you do not specify an interface, the output of the command shows the status on all switch ports:

```
Switch# show interfaces transceiver properties
Name : Fa0/1
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: on

Name : Fa0/2
Administrative Speed: auto
Administrative Duplex: auto
Administrative Auto-MDIX: on
Administrative Power Inline: N/A
Operational Speed: 100
Operational Duplex: full
Operational Auto-MDIX: on

<output truncated>
```

**Related Commands**

| Command | Description |
|---|---|
| **switchport access vlan** | Configures a port as a static-access or a dynamic-access port. |
| **switchport block** | Blocks unknown unicast or multicast traffic on an interface. |
| **switchport mode** | Configures the VLAN membership mode of a port. |
| **switchport mode private-vlan** | Configures a port as a private-VLAN host or a promiscuous port. |
| **switchport mode private-vlan** | Defines private-VLAN association for a host port or private-VLAN mapping for a promiscuous port. |

# show interfaces counters

Use the **show interfaces counters** privileged EXEC command to display various counters for the switch or for a specific interface.

**show interfaces** [*interface-id* | **vlan** *vlan-id*] **counters** [**errors** | **trunk**] [**module** *switch- number*] | **etherchannel** | **protocol status**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) ID of the physical interface, including type, module, and port number. |
| **errors** | (Optional) Display error counters. |
| **trunk** | (Optional) Display trunk counters. |
| **module** *switch- number* | **Note** (Optional) Display counters for the specified switch number. The only available value is 1. |
| **etherchannel** | (Optional) Display EtherChannel counters, including octets, broadcast packets, multicast packets, and unicast packets received and sent. |
| **protocol status** | (Optional) Display status of protocols enabled on interfaces. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help string, the **vlan** *vlan-id* keyword is not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not enter any keywords, all counters for all interfaces are included.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of partial output from the **show interfaces counters** command. It displays all counters for the switch.

```
Switch# show interfaces counters
Port            InOctets    InUcastPkts    InMcastPkts    InBcastPkts
Fa0/1                  0              0              0              0
Fa0/2                  0              0              0              0

<output truncated>
```

This is an example of partial output from the **show interfaces counters protocol status** command for all interfaces.

```
Switch# show interfaces counters protocol status
Protocols allocated:
 Vlan1: Other, IP
 Vlan20: Other, IP, ARP
 Vlan30: Other, IP, ARP
 Vlan40: Other, IP, ARP
 Vlan50: Other, IP, ARP
 Vlan60: Other, IP, ARP
 Vlan70: Other, IP, ARP
 Vlan80: Other, IP, ARP
 Vlan90: Other, IP, ARP
 Vlan900: Other, IP, ARP
 Vlan3000: Other, IP
 Vlan3500: Other, IP
 FastEthernet0/1: Other, IP, ARP, CDP
 FastEthernet0/2: Other, IP
 FastEthernet0/3: Other, IP
 FastEthernet0/4: Other, IP
 FastEthernet0/5: Other, IP
 FastEthernet0/6: Other, IP
 FastEthernet0/7: Other, IP
 FastEthernet0/8: Other, IP
 FastEthernet0/9: Other, IP
 FastEthernet0/10: Other, IP, CDP

<output truncated>
```

This is an example of output from the **show interfaces counters trunk** command. It displays trunk counters for all interfaces.

```
Switch# show interfaces counters trunk
Port        TrunkFramesTx  TrunkFramesRx  WrongEncap
Gi0/1               0              0           0
Gi0/2               0              0           0
Gi0/3           80678           4155           0
Gi0/4           82320            126           0
Gi0/5               0              0           0

<output truncated>
```

## Related Commands

| Command | Description |
|---|---|
| **show interfaces** | Displays additional interface characteristics. |

# show inventory

Use the **show inventory** user EXEC command to display product identification (PID) information for the hardware.

**show inventory** [*entity-name* | **raw**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *entity-name* | (Optional) Display the specified entity. For example, enter the interface (such as gigabitethernet 0/x) into which a small form-factor pluggable (SFP) module is installed to display its identity. |
| **raw** | (Optional) Display every entity in the device. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG1 | Support for the *entity-name* keyword was added. |

## Usage Guidelines

The command is case sensitive. With no arguments, the **show inventory** command produces a compact display of all identifiable entities that have a product identifier. The display shows the entity location (slot identity), entity description, and the unique device identifier (UDI), including PID, version identifier (VID), and serial number (SN) of that entity.

Many legacy SFPs are not programmed with PIDs and VID.s

**Note** If there is no PID, no output appears when you enter the **show inventory** command.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is example output from the **show inventory** command:

```
Switch> show inventory
NAME: "1", DESCR: "ME-2400-24TS-A"
PID: ME-2400-24TS-A , VID:Vo1 , SN: FHH0914002G

NAME: "GigabitEthernet0/1", DESCR: "100BaseBX-10U SFP"
PID:                      , VID:    , SN: NEC08440067

NAME: "GigabitEthernet0/2", DESCR: "10/100/1000BaseTX SFP"
PID:                      , VID:    , SN: 00000MTC0839048G
```

# show ip dhcp snooping

Use the **show ip dhcp snooping** user EXEC command to display the DHCP snooping configuration.

**show ip dhcp snooping** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show ip dhcp snooping** command.

```
Switch> show ip dhcp snooping
Switch DHCP snooping is enabled
DHCP snooping is configured on following VLANs:
40-42
Insertion of option 82 is enabled
Option 82 on untrusted port is allowed
Verification of hwaddr field is enabled
Interface                    Trusted     Rate limit (pps)
------------------------     -------     ----------------
GigabitEthernet0/1               yes         unlimited
GigabitEthernet0/2               yes         unlimited
```

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |

# show ip dhcp snooping binding

Use the **show ip dhcp snooping binding** user EXEC command to display the DHCP snooping binding database and configuration information for all interfaces on a switch.

**show ip dhcp snooping binding** [*ip-address*] [*mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) Specify the binding entry IP address. |
| *mac-address* | (Optional) Specify the binding entry MAC address. |
| **interface** *interface-id* | (Optional) Specify the binding input interface. |
| **vlan** *vlan-id* | (Optional) Specify the binding entry VLAN. |
| **\| begin** | Display begins with the line that matches the *expression*. |
| **\| exclude** | Display excludes lines that match the *expression*. |
| **\| include** | Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **show ip dhcp snooping binding** command output shows the dynamically configured bindings.

If DHCP snooping is enabled and an interface changes to the down state, the switch does not delete the statically configured bindings.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This example shows how to display the DHCP snooping binding entries for a switch:

```
Switch> show ip dhcp snooping binding
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9837        dhcp-snooping  20    GigabitEthernet0/1
00:D0:B7:1B:35:DE   10.1.2.151       237         dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 2
```

This example shows how to display the DHCP snooping binding entries for a specific IP address:

```
Switch> show ip dhcp snooping binding 10.1.2.150
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9810        dhcp-snooping  20    GigabitEthernet0/1
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries for a specific MAC address:

```
Switch> show ip dhcp snooping binding 0102.0304.0506
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9788        dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on a port:

```
Switch> show ip dhcp snooping binding interface gigabitethernet0/2
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
00:30:94:C2:EF:35   10.1.2.151       290         dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 1
```

This example shows how to display the DHCP snooping binding entries on VLAN 20:

```
Switch> show ip dhcp snooping binding vlan 20
MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  --------------------
01:02:03:04:05:06   10.1.2.150       9747        dhcp-snooping  20    GigabitEthernet0/1
00:00:00:00:00:02   10.1.2.151       65          dhcp-snooping  20    GigabitEthernet0/2
Total number of bindings: 2
```

Table 2-11 describes the fields in the **show ip dhcp snooping binding** command output:

***Table 2-11 show ip dhcp snooping binding Command Output***

| Field | Description |
|---|---|
| MacAddress | Client hardware MAC address |
| IpAddress | Client IP address assigned from the DHCP server |
| Lease(sec) | Remaining lease time for the IP address |
| Type | Binding type |
| VLAN | VLAN number of the client interface |
| Interface | Interface that connects to the DHCP client host |
| Total number of bindings | Total number of bindings configured on the switch<br>**Note** The command output might not show the total number of bindings. For example, if 200 bindings are configured on the switch and you stop the display before all the bindings appear, the total number does not change. |

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping binding** | Configures the DHCP snooping binding database |
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |

# show ip dhcp snooping database

Use the **show ip dhcp snooping database** user EXEC command to display the status of the DHCP snooping binding database agent.

**show ip dhcp snooping database** [**detail**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Display detailed status and statistics information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This is an example of output from the **show ip dhcp snooping database** command:

```
Switch> show ip dhcp snooping database
Agent URL :
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        0   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0
```

This is an example of output from the **show ip dhcp snooping database detail** command:

```
Switch# show ip dhcp snooping database detail
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : No
Delay Timer Expiry : 7 (00:00:07)
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : 17:14:25 UTC Sat Jul 7 2001
Last Failed Reason : Unable to access URL.

Total Attempts       :       21   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :       21
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :       21
Media Failures       :        0

First successful access: Read

Last ignored bindings counters :
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
Last Ignored Time : None

Total ignored bindings counters:
Binding Collisions    :        0   Expired leases    :        0
Invalid interfaces    :        0   Unsupported vlans :        0
Parse failures        :        0
```

## Related Commands

| Command | Description |
|---|---|
| **ip dhcp snooping** | Enables DHCP snooping on a VLAN. |
| **ip dhcp snooping database** | Configures the DHCP snooping binding database agent or the binding file. |
| **show ip dhcp snooping** | Displays DHCP snooping information. |

# show ip dhcp snooping statistics

Use the **show ip dhcp snooping statistics** user EXEC command to display DHCP snooping statistics in summary or detail form.

**show ip dhcp snooping statistics** [**detail**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Display detailed statistics information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(37)SE | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

In a switch stack, all statistics are generated on the stack master. If a new stack master is elected, the statistics counters reset.

## Examples

This is an example of output from the **show ip dhcp snooping statistics** command:

```
Switch> show ip dhcp snooping statistics
 Packets Forwarded                                = 0
 Packets Dropped                                  = 0
 Packets Dropped From untrusted ports             = 0
```

This is an example of output from the **show ip dhcp snooping statistics detail** command:

```
Switch> show ip dhcp snooping statistics detail
 Packets Processed by DHCP Snooping               = 0
 Packets Dropped Because
   IDB not known                                  = 0
   Queue full                                     = 0
   Interface is in errdisabled                    = 0
   Rate limit exceeded                            = 0
   Received on untrusted ports                    = 0
   Nonzero giaddr                                 = 0
   Source mac not equal to chaddr                 = 0
   Binding mismatch                               = 0
   Insertion of opt82 fail                        = 0
   Interface Down                                 = 0
   Unknown output interface                       = 0
   Reply output port equal to input port          = 0
   Packet denied by platform                      = 0
```

Table 2-12 shows the DHCP snooping statistics and their descriptions:

*Table 2-12 DHCP Snooping Statistics*

| DHCP Snooping Statistic | Description |
|---|---|
| Packets Processed by DHCP Snooping | Total number of packets handled by DHCP snooping, including forwarded and dropped packets. |
| Packets Dropped Because IDB not known | Number of errors when the input interface of the packet cannot be determined. |
| Queue full | Number of errors when an internal queue used to process the packets is full. This might happen if DHCP packets are received at an excessively high rate and rate limiting is not enabled on the ingress ports. |
| Interface is in errdisabled | Number of times a packet was received on a port that has been marked as error disabled. This might happen if packets are in the processing queue when a port is put into the error-disabled state and those packets are subsequently processed. |
| Rate limit exceeded | Number of times the rate limit configured on the port was exceeded and the interface was put into the error-disabled state. |
| Received on untrusted ports | Number of times a DHCP server packet (OFFER, ACK, NAK, or LEASEQUERY) was received on an untrusted port and was dropped. |
| Nonzero giaddr | Number of times the relay agent address field (giaddr) in the DHCP packet received on an untrusted port was not zero, or the **no ip dhcp snooping information option allow-untrusted** global configuration command is not configured and a packet received on an untrusted port contained option-82 data. |
| Source mac not equal to chaddr | Number of times the client MAC address field of the DHCP packet (chaddr) does not match the packet source MAC address and the **ip dhcp snooping verify mac-address** global configuration command is configured. |
| Binding mismatch | Number of times a RELEASE or DECLINE packet was received on a port that is different than the port in the binding for that MAC address-VLAN pair. This indicates someone might be trying to spoof the real client, or it could mean that the client has moved to another port on the switch and issued a RELEASE or DECLINE. The MAC address is taken from the chaddr field of the DHCP packet, not the source MAC address in the Ethernet header. |

*Table 2-12 DHCP Snooping Statistics*

| DHCP Snooping Statistic | Description |
|---|---|
| Insertion of opt82 fail | Number of times the option-82 insertion into a packet failed. The insertion might fail if the packet with the option-82 data exceeds the size of a single physical packet on the internet. |
| Interface Down | Number of times the packet is a reply to the DHCP relay agent, but the SVI interface for the relay agent is down. This is an unlikely error that occurs if the SVI goes down between sending the client request to the DHCP server and receiving the response. |
| Unknown output interface | Number of times the output interface for a DHCP reply packet cannot be determined by either option-82 data or a lookup in the MAC address table. The packet is dropped. This can happen if option 82 is not used and the client MAC address has aged out. If IPSG is enabled with the port-security option and option 82 is not enabled, the MAC address of the client is not learned, and the reply packets will be dropped. |
| Reply output port equal to input port | Number of times the output port for a DHCP reply packet is the same as the input port, causing a possible loop. Indicates a possible network misconfiguration or misuse of trust settings on ports. |
| Packet denied by platform | Number of times the packet has been denied by a platform-specific registry. |

## Related Commands

| Command | Description |
|---|---|
| **clear ip dhcp snooping** | Clears the DHCP snooping binding database, the DHCP snooping binding database agent statistics, or the DHCP snooping statistics counters. |

# show ip igmp profile

Use the **show ip igmp profile** privileged EXEC command to display all configured Internet Group Management Protocol (IGMP) profiles or a specified IGMP profile.

**show ip igmp profile** [*profile number*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *profile number* | (Optional) The IGMP profile number to be displayed. The range is 1 to 4294967295. If no profile number is entered, all IGMP profiles are displayed. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

These are examples of output from the **show ip igmp profile** privileged EXEC command, with and without specifying a profile number. If no profile number is entered, the display includes all profiles configured on the switch.

```
Switch# show ip igmp profile 40
IGMP Profile 40
    permit
    range 233.1.1.1 233.255.255.255

Switch# show ip igmp profile
IGMP Profile 3
    range 230.9.9.0 230.9.9.0
IGMP Profile 4
    permit
    range 229.9.9.0 229.255.255.255
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp profile** | Configures the specified IGMP profile number. |

# show ip igmp snooping

Use the **show ip igmp snooping** user EXEC command to display the Internet Group Management Protocol (IGMP) snooping configuration of the switch or the VLAN.

**show ip igmp snooping** [**groups** | **mrouter** | **querier** [**vlan** *vlan-id*] **[detail]** ] [**vlan** *vlan-id*] **[detail]** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **groups** | (Optional) See the **show ip igmp snooping groups** command. |
| **mrouter** | (Optional) See the **show ip igmp snooping mrouter** command. |
| **querier** | (Optional) See the **show ip igmp snooping querier** command. |
| **vlan** *vlan-id* | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094 (available only in privileged EXEC mode). |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to display snooping configuration for the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Although visible in the output display, output lines for source-only learning are not valid.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show ip igmp snooping vlan 1** command. It shows snooping characteristics for a specific VLAN.

```
Switch# show ip igmp snooping vlan 1
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             :Enabled
IGMPv3 snooping (minimal) :Enabled
Report suppression        :Enabled
TCN solicit query         :Disabled
TCN flood query count     :2
Last member query interval : 100
```

```
Vlan 1:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval : 100
```

**Note** Source-only learning are not supported, and information appearing for this feature is not valid.

This is an example of output from the **show ip igmp snooping** command. It displays snooping characteristics for all VLANs on the switch.

```
Switch> show ip igmp snooping
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping              : Enabled
IGMPv3 snooping (minimal)  : Enabled
Report suppression         : Enabled
TCN solicit query          : Disabled
TCN flood query count      : 2
Last member query interval : 100

Vlan 1:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 100

Vlan 2:
--------
IGMP snooping                          :Enabled
Immediate leave                        :Disabled
Multicast router learning mode         :pim-dvmrp
Source only learning age timer         :10
CGMP interoperability mode             :IGMP_ONLY
Last member query interval             : 333

<output truncated>
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping | Enables and configures IGMP snooping on the switch or on a VLAN. |
| show ip igmp snooping mrouter | Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN. |
| show ip igmp snooping querier | Displays the configuration and operation information for the IGMP querier configured on a switch. |

# show ip igmp snooping groups

Use the **show ip igmp snooping groups** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping multicast table for the switch or the multicast information. Use with the **vlan** keyword to display the multicast table for a specified multicast VLAN or specific multicast information.

**show ip igmp snooping groups** [**count** | **dynamic** [**count**] | **user** [**count**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show ip igmp snooping groups vlan** *vlan-id* [*ip_address* | **count** | **dynamic** [**count**] | **user** [**count**]] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **count** | (Optional) Display the total number of entries for the specified command options instead of the actual entries. |
| **dynamic** | (Optional) Display entries learned by IGMP snooping. |
| **user** | Optional) Display only the user-configured multicast entries. |
| **ip_address** | (Optional) Display characteristics of the multicast group with the specified group IP address. |
| *vlan-id* | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to display multicast information or the multicast table.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show ip igmp snooping groups** command without any keywords. It displays the multicast table for the switch.

```
Switch# show ip igmp snooping groups
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Gi0/2
104       224.1.4.3       igmp        v2          Gi0/1, Gi0/2
```

This is an example of output from the **show ip igmp snooping groups count** command. It displays the total number of multicast groups on the switch.

```
Switch# show ip igmp snooping groups count
Total number of multicast groups: 2
```

This is an example of output from the **show ip igmp snooping groups dynamic** command. It shows only the entries learned by IGMP snooping.

```
Switch# show ip igmp snooping groups vlan 1 dynamic
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Fa0/15
104       224.1.4.3       igmp        v2          Gi0/1, Fa0/15
```

This is an example of output from the **show ip igmp snooping groups vlan** *vlan-id ip-address* command. It shows the entries for the group with the specified IP address.

```
Switch# show ip igmp snooping groups vlan 104 224.1.4.2
Vlan      Group           Type        Version     Port List
------------------------------------------------------------
104       224.1.4.2       igmp        v2          Gi0/1, Fa0/15
```

## Related Commands

| Command | Description |
|---|---|
| **ip igmp snooping** | Enables and configures IGMP snooping on the switch or on a VLAN. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration of the switch or the VLAN. |
| **show ip igmp snooping mrouter** | Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN. |

# show ip igmp snooping mrouter

Use the **show ip igmp snooping mrouter** privileged EXEC command to display the Internet Group Management Protocol (IGMP) snooping dynamically learned and manually configured multicast router ports for the switch or for the specified multicast VLAN.

**show ip igmp snooping mrouter** [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to display multicast router ports on the switch or for a specific VLAN.

VLAN IDs 1002 to 1005 are reserved for Token Ring and FDDI VLANs and cannot be used in IGMP snooping.

When multicast VLAN registration (MVR) is enabled, the **show ip igmp snooping mrouter** command displays MVR multicast router information and IGMP snooping information.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show ip igmp snooping mrouter** command. It shows how to display multicast router ports on the switch.

```
Switch# show ip igmp snooping mrouter
Vlan    ports
----    -----
   1    Gi0/1(dynamic)
```

**Related Commands**

| Command | Description |
|---|---|
| **ip igmp snooping** | Enables and configures IGMP snooping on the switch or on a VLAN. |
| **ip igmp snooping vlan mrouter** | Adds a multicast router port to a multicast VLAN. |
| **show ip igmp snooping** | Displays the IGMP snooping configuration of the switch or the VLAN. |
| **show ip igmp snooping groups** | Displays IGMP snooping multicast information for the switch or for the specified parameter. |

# show ip igmp snooping querier

Use the **show ip igmp snooping querier** user EXEC command to display the IP address and incoming port for the Internet Group Management Protocol (IGMP) query most recently received by the switch.

**show ip igmp snooping querier** [**vlan** *vlan-id*] **[detail]** [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Specify a VLAN; the range is 1 to 1001 and 1006 to 4094. |
| **detail** | (Optional) Display querier information as well as configuration and operational information pertaining to the querier. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **show ip igmp snooping querier** command to display the IGMP version and IP address of a detected device (also called a *querier*) that sends IGMP query message. A subnet can have multiple multicast routers but has only one IGMP querier. In a subnet running IGMPv2, one of the multicast routers is elected as the querier. The querier can be a Layer 3 switch.

The **show ip igmp snooping querier** command output also shows the VLAN and interface on which the querier was detected. If the querier is the switch, the output shows the *Port* field as *Router.* If the querier is a router, the output shows the port number on which the querier is learned in the *Port* field.

The **show ip igmp snooping querier detail** user EXEC command is similar to the **show ip igmp snooping querier** command. However, the **show ip igmp snooping querier detail** command displays the IP address of the most recent device detected by the switch querier along with this additional information:

- The elected IGMP querier in the VLAN
- The configuration and operational information pertaining to the switch querier (if any) that is configured in the VLAN

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show ip igmp snooping querier** command:

```
Switch> show ip igmp snooping querier
Vlan      IP Address     IGMP Version        Port
--------------------------------------------------
1         172.20.50.11   v3                  Gi0/1
2         172.20.40.20   v2                  Router
```

This is an example of output from the **show ip igmp snooping querier detail** command:

```
Switch> show ip igmp snooping querier detail

Vlan      IP Address     IGMP Version   Port
-----------------------------------------------------------
1         1.1.1.1        v2             Fa0/1

Global IGMP switch querier status
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 0.0.0.0
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10

Vlan 1:   IGMP switch querier status

-----------------------------------------------------------
elected querier is 1.1.1.1         on port Fa0/1
-----------------------------------------------------------
admin state                    : Enabled
admin version                  : 2
source IP address              : 10.1.1.65
query-interval (sec)           : 60
max-response-time (sec)        : 10
querier-timeout (sec)          : 120
tcn query count                : 2
tcn query interval (sec)       : 10
operational state              : Non-Querier
operational version            : 2
tcn query pending count        : 0
```

## Related Commands

| Command | Description |
|---|---|
| ip igmp snooping querier | Enables and configures the IGMP snooping querier on the switch or on a VLAN. |
| show ip igmp snooping mrouter | Displays IGMP snooping multicast router ports for the switch or for the specified multicast VLAN. |

# show lacp

Use the **show lacp** user EXEC command to display Link Aggregation Control Protocol (LACP) channel-group information.

**show lacp** [*channel-group-number*] {**counters** | **internal** | **neighbor** | **sys-id**} [ | {**begin** | **exclude** | **include**} *expression*]

**Note** LACP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *channel-group-number* | (Optional) Number of the channel group. The range is 1 to 48. |
| **counters** | Display traffic information. |
| **internal** | Display internal information. |
| **neighbor** | Display neighbor information. |
| **sys-id** | Display the system identifier that is being used by LACP. The system identifier is made up of the LACP system priority and the switch MAC address. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can enter any **show lacp** command to display the active channel-group information. To display specific channel information, enter the **show lacp** command with a channel-group number.

If you do not specify a channel group, information for all channel groups appears.

You can enter the *channel-group-number* option to specify a channel group for all keywords except **sys-id**.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show lacp counters** user EXEC command. Table 2-13 describes the fields in the display.

```
Switch> show lacp counters
               LACPDUs          Marker      Marker Response    LACPDUs
Port          Sent    Recv     Sent    Recv     Sent    Recv      Pkts Err
--------------------------------------------------------------------------
Channel group:1
Gi0/1         19      10       0       0        0       0         0
Gi0/2         14      6        0       0        0       0         0
```

*Table 2-13 show lacp counters Field Descriptions*

| Field | Description |
|---|---|
| LACPDUs Sent and Recv | The number of LACP packets sent and received by a port. |
| Marker Sent and Recv | The number of LACP marker packets sent and received by a port. |
| Marker Response Sent and Recv | The number of LACP marker response packets sent and received by a port. |
| LACPDUs Pkts and Err | The number of unknown and illegal packets received by LACP for a port. |

This is an example of output from the **show lacp internal** command:

```
Switch> show lacp 1 internal
Flags:  S - Device is requesting Slow LACPDUs
        F - Device is requesting Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 1
                            LACP port     Admin     Oper    Port     Port
Port        Flags   State   Priority      Key       Key     Number   State
Gi0/1       SA      bndl    32768         0x3       0x3     0x4      0x3D
Gi0/2       SA      bndl    32768         0x3       0x3     0x5      0x3D
```

Table 2-14 describes the fields in the display.

*Table 2-14 show lacp internal Field Descriptions*

| Field | Description |
|---|---|
| State | State of the specific port. These are the allowed values:<br>• – —Port is in an unknown state.<br>• **bndl**—Port is attached to an aggregator and bundled with other ports.<br>• **susp**—Port is in a suspended state; it is not attached to any aggregator.<br>• **hot-sby**—Port is in a hot-standby state.<br>• **indiv**—Port is incapable of bundling with any other port.<br>• **indep**—Port is in an independent state (not bundled but able to switch data traffic. In this case, LACP is not running on the partner port).<br>• **down**—Port is down. |
| LACP Port Priority | Port priority setting. LACP uses the port priority to put ports s in standby mode when there is a hardware limitation that prevents all compatible ports from aggregating. |
| Admin Key | Administrative key assigned to this port. LACP automatically generates an administrative key value as a hexadecimal number. The administrative key defines the ability of a port to aggregate with other ports. A port's ability to aggregate with other ports is determined by the port physical characteristics (for example, data rate and duplex capability) and configuration restrictions that you establish. |
| Oper Key | Runtime operational key that is being used by this port. LACP automatically generates this value as a hexadecimal number. |
| Port Number | Port number. |
| Port State | State variables for the port, encoded as individual bits within a single octet with these meanings:<br>• bit0: LACP_Activity<br>• bit1: LACP_Timeout<br>• bit2: Aggregation<br>• bit3: Synchronization<br>• bit4: Collecting<br>• bit5: Distributing<br>• bit6: Defaulted<br>• bit7: Expired<br>**Note** In the above list, bit7 is the MSB and bit0 is the LSB. |

This is an example of output from the **show lacp neighbor** command:

```
Switch> show lacp neighbor
Flags:  S - Device is sending Slow LACPDUs F - Device is sending Fast LACPDUs
        A - Device is in Active mode       P - Device is in Passive mode

Channel group 3 neighbors

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/1     32768,0007.eb49.5e80  0xC               19s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C

Partner's information:

          Partner               Partner                     Partner
Port      System ID             Port Number     Age         Flags
Gi0/2     32768,0007.eb49.5e80  0xD               15s       SP

          LACP Partner          Partner         Partner
          Port Priority         Oper Key        Port State
          32768                 0x3             0x3C
```

This is an example of output from the **show lacp sys-id** command:

```
Switch> show lacp sys-id
32765,0002.4b29.3a00
```

The system identification is made up of the system priority and the system MAC address. The first two bytes are the system priority, and the last six bytes are the globally administered individual MAC address associated to the system.

## Related Commands

| Command | Description |
|---|---|
| **clear lacp** | Clears the LACP channel-group information. |
| **lacp port-priority** | Configures the LACP port priority. |
| **lacp system-priority** | Configures the LACP system priority. |

# show mac access-group

Use the **show mac access-group** user EXEC command to display the MAC access control lists (ACLs) configured for an interface or a switch.

**show mac access-group** [**interface** *interface-id*] [ | {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Display the MAC ACLs configured on a specific interface. Valid interfaces are physical ports and port channels; the port-channel range is 1 to 48 (available only in privileged EXEC mode). |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac-access group** user EXEC command. In this display, Fast Ethernet interface 0/2 has the MAC access list *macl_e1* applied to inbound traffic; no MAC ACLs are applied to other interfaces.

```
Switch> show mac access-group
Interface FastEthernet0/1:
   Inbound access-list is macl_e1
   Outbound access-list is not set
Interface FastEthernet0/2:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernet0/3:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernet0/4:
   Inbound access-list is not set
   Outbound access-list is not set
Interface FastEthernetv0/5:
   Inbound access-list is not set
   Outbound access-list is not set
<output truncated>
```

This is an example of output from the **show mac access-group interface fastethernet0/1** command:

```
Switch# show mac access-group interface fastethernet0/1
Interface FastEthernet0/1:
   Inbound access-list is macl_e1
```

**Related Commands**

| Command | Description |
|---|---|
| **mac access-group** | Applies a MAC access group to an interface. |

# show mac address-table

Use the **show mac address-table** user EXEC command to display a specific MAC address table static and dynamic entry or the MAC address table static and dynamic entries on a specific interface or VLAN.

**show mac address-table** [ **|** {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table** command:

```
Switch> show mac address-table
          Mac Address Table
-------------------------------------------
Vlan    Mac Address       Type       Ports
----    -----------       ----       -----
 All    0000.0000.0001    STATIC     CPU
 All    0000.0000.0002    STATIC     CPU
 All    0000.0000.0003    STATIC     CPU
 All    0000.0000.0009    STATIC     CPU
 All    0000.0000.0012    STATIC     CPU
 All    0180.c200.000b    STATIC     CPU
 All    0180.c200.000c    STATIC     CPU
 All    0180.c200.000d    STATIC     CPU
 All    0180.c200.000e    STATIC     CPU
 All    0180.c200.000f    STATIC     CPU
 All    0180.c200.0010    STATIC     CPU
   1    0030.9441.6327    DYNAMIC    Gi0/4
Total Mac Addresses for this criterion: 12
```

## Related Commands

| Command | Description |
|---|---|
| **clear mac address-table dynamic** | Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table address

Use the **show mac address-table address** user EXEC command to display MAC address table information for the specified MAC address.

**show mac address-table address** *mac-address* [**interface** *interface-id*] [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *mac-address* | Specify the 48-bit MAC address; the valid format is H.H.H. |
| **interface** *interface-id* | (Optional) Display information for a specific interface. Valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Display entries for the specific VLAN only. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table address** command:

```
Switch# show mac address-table address 0002.4b28.c482
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0002.4b28.c482  STATIC  CPU
Total Mac Addresses for this criterion: 1
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table aging-time

Use the **show mac address-table aging-time** user EXEC command to display the aging time of a specific address table instance, all address table instances on a specified VLAN or, if a specific VLAN is not specified, on all VLANs.

**show mac address-table aging-time** [**vlan** *vlan-id*] [ **|** {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Display aging time information for a specific VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If no VLAN number is specified, the aging time for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table aging-time** command:

```
Switch> show mac address-table aging-time
Vlan    Aging Time
----    ----------
   1     300
```

This is an example of output from the **show mac address-table aging-time vlan 10** command:

```
Switch> show mac address-table aging-time vlan 10
Vlan    Aging Time
----    ----------
  10     300
```

## Related Commands

| Command | Description |
|---|---|
| **mac address-table aging-time** | Sets the length of time that a dynamic entry remains in the MAC address table after the entry is used or updated. |
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table count

Use the **show mac address-table count** user EXEC command to display the number of addresses present in all VLANs or the specified VLAN.

**show mac address-table count** [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) Display the number of addresses for a specific VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If no VLAN number is specified, the address count for all VLANs appears.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table count** command:

```
Switch# show mac address-table count
Mac Entries for Vlan   : 1
---------------------------
Dynamic Address Count  : 2
Static  Address Count  : 0
Total Mac Addresses    : 2
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table dynamic

Use the **show mac address-table dynamic** user EXEC command to display only dynamic MAC address table entries.

**show mac address-table dynamic** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **address** *mac-address* | (Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only). |
| **interface** *interface-id* | (Optional) Specify an interface to match; valid *interfaces* include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Display entries for a specific VLAN; the range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table dynamic** command:

```
Switch> show mac address-table dynamic
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

## Related Commands

| Command | Description |
|---|---|
| **clear mac address-table dynamic** | Deletes from the MAC address table a specific dynamic address, all dynamic addresses on a particular interface, or all dynamic addresses on a particular VLAN. |
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table interface

Use the **show mac address-table interface** user command to display the MAC address table information for the specified interface in the specified VLAN.

**show mac address-table interface** *interface-id* [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | Specify an interface type; valid interfaces include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Display entries for a specific VLAN; the range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table interface** command:

```
Switch> show mac address-table interface gigabitethernet0/2
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0030.b635.7862  DYNAMIC Gi0/2
   1    00b0.6496.2741  DYNAMIC Gi0/2
Total Mac Addresses for this criterion: 2
```

## Related Commands

| Command | Description |
|---|---|
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table notification

Use the **show mac address-table notification** user EXEC command to display the MAC address notification settings for all interfaces or the specified interface.

**show mac address-table notification** [**interface** [*interface-id*]] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** | (Optional) Display information for all interfaces. Valid interfaces include physical ports and port channels. |
| *interface-id* | (Optional) Display information for the specified interface. Valid interfaces include physical ports and port channels. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **show mac address-table notification** command without any keywords to display whether the feature is enabled or disabled, the MAC notification interval, the maximum number of entries allowed in the history table, and the history table contents.

Use the **interface** keyword to display the flags for all interfaces. If the *interface-id* is included, only the flags for that interface appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table notification** command:

```
Switch> show mac address-table notification
MAC Notification Feature is Enabled on the switch
Interval between Notification Traps : 60 secs
Number of MAC Addresses Added : 4
Number of MAC Addresses Removed : 4
Number of Notifications sent to NMS : 3
Maximum Number of entries configured in History Table : 100
Current History Table Length : 3
MAC Notification Traps are Enabled
History Table contents
----------------------
History Index 0, Entry Timestamp 1032254, Despatch Timestamp 1032254
MAC Changed Message :
```

```
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1

History Index 1, Entry Timestamp 1038254, Despatch Timestamp 1038254
MAC Changed Message :
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Added   Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1

History Index 2, Entry Timestamp 1074254, Despatch Timestamp 1074254
MAC Changed Message :
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0000 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0001 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0002 Module: 0   Port: 1
Operation: Deleted Vlan: 2     MAC Addr: 0000.0000.0003 Module: 0   Port: 1
```

## Related Commands

| Command | Description |
|---|---|
| **clear mac address-table notification** | Clears the MAC address notification global counters. |
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |
| **show mac address-table vlan** | Displays the MAC address table information for the specified VLAN. |

# show mac address-table static

Use the **show mac address-table static** user EXEC command to display only static MAC address table entries.

**show mac address-table static** [**address** *mac-address*] [**interface** *interface-id*] [**vlan** *vlan-id*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **address** *mac-address* | (Optional) Specify a 48-bit MAC address; the valid format is H.H.H (available in privileged EXEC mode only). |
| **interface** *interface-id* | (Optional) Specify an interface to match; valid *interfaces* include physical ports and port channels. |
| **vlan** *vlan-id* | (Optional) Display addresses for a specific VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table static** command:

```
Switch> show mac address-table static
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
 All    0100.0ccc.cccc  STATIC  CPU
 All    0180.c200.0000  STATIC  CPU
 All    0100.0ccc.cccd  STATIC  CPU
 All    0180.c200.0001  STATIC  CPU
 All    0180.c200.0004  STATIC  CPU
 All    0180.c200.0005  STATIC  CPU
   4    0001.0002.0004  STATIC  Drop
   6    0001.0002.0007  STATIC  Drop
Total Mac Addresses for this criterion: 8
```

## Related Commands

| Command | Description |
|---|---|
| mac address-table static | Adds static addresses to the MAC address table. |
| mac address-table static drop | Enables unicast MAC address filtering and configures the switch to drop traffic with a specific source or destination MAC address. |
| show mac address-table address | Displays MAC address table information for the specified MAC address. |
| show mac address-table aging-time | Displays the aging time in all VLANs or the specified VLAN. |
| show mac address-table count | Displays the number of addresses present in all VLANs or the specified VLAN. |
| show mac address-table dynamic | Displays dynamic MAC address table entries only. |
| show mac address-table interface | Displays the MAC address table information for the specified interface. |
| show mac address-table notification | Displays the MAC address notification settings for all interfaces or the specified interface. |
| show mac address-table vlan | Displays the MAC address table information for the specified VLAN. |

# show mac address-table vlan

Use the **show mac address-table vlan** user EXEC command to display the MAC address table information for the specified VLAN.

**show mac address-table vlan** *vlan-id* [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *vlan-id* | (Optional) Display addresses for a specific VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mac address-table vlan 1** command:

```
Switch> show mac address-table vlan 1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address     Type    Ports
----    -----------     ----    -----
   1    0100.0ccc.cccc  STATIC  CPU
   1    0180.c200.0000  STATIC  CPU
   1    0100.0ccc.cccd  STATIC  CPU
   1    0180.c200.0001  STATIC  CPU
   1    0180.c200.0002  STATIC  CPU
   1    0180.c200.0003  STATIC  CPU
   1    0180.c200.0005  STATIC  CPU
   1    0180.c200.0006  STATIC  CPU
   1    0180.c200.0007  STATIC  CPU
Total Mac Addresses for this criterion: 9
```

**Related Commands**

| Command | Description |
|---|---|
| **show mac address-table address** | Displays MAC address table information for the specified MAC address. |
| **show mac address-table aging-time** | Displays the aging time in all VLANs or the specified VLAN. |
| **show mac address-table count** | Displays the number of addresses present in all VLANs or the specified VLAN. |
| **show mac address-table dynamic** | Displays dynamic MAC address table entries only. |
| **show mac address-table interface** | Displays the MAC address table information for the specified interface. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or the specified interface. |
| **show mac address-table static** | Displays static MAC address table entries only. |

# show monitor

Use the **show monitor** user EXEC command to display information about all Switched Port Analyzer (SPAN) and Remote SPAN (RSPAN) sessions on the switch. Use the command with keywords to show a specific session, all sessions, all local sessions, or all remote sessions.

**show monitor** [**session** {*session_number* | **all** | **local** | **range** *list* | **remote**} [**detail**]] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **session** | (Optional) Display information about specified SPAN sessions. |
| *session_number* | Specify the number of the SPAN or RSPAN session. The range is 1 to 66. |
| **all** | Display all SPAN sessions. |
| **local** | Display only local SPAN sessions. |
| **range** *list* | Display a range of SPAN sessions, where *list* is the range of valid sessions, either a single session or a range of sessions described by two numbers, the lower one first, separated by a hyphen. Do not enter any spaces between comma-separated parameters or in hyphen-specified ranges.<br>**Note** This keyword is available only in privileged EXEC mode. |
| **remote** | Display only remote SPAN sessions. |
| **detail** | (Optional) Display detailed information about the specified sessions. |
| **\| begin** | Display begins with the line that matches the *expression*. |
| **\| exclude** | Display excludes lines that match the *expression*. |
| **\| include** | Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

The output is the same for the **show monitor** command and the **show monitor session all** command.

## Examples

This is an example of output for the **show monitor** user EXEC command:

```
Switch# show monitor
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa0/24
    TX Only:      None
    Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
    Encapsulation:Replicate

Session 2
---------
 Type       :Remote Source Session
Source Ports:
Source VLANs:
TX Only:      10
    Both:         1-9
Dest RSPAN VLAN:  105
```

This is an example of output for the **show monitor** user EXEC command for RSPAN source session 1:

```
Switch# show monitor session 1
Session 1
---------
 Type       :Local Session
Source Ports:
    RX Only:      Fa0/24
    TX Only:      None
    Both:         Fa0/1-2,Fa0/1-5
Destination Ports:Fa0/18
    Encapsulation:Replicate
```

This is an example of output for the **show monitor session all** user EXEC command when ingress traffic forwarding is enabled:

```
Switch# show monitor session all
Session 1
---------
Type               :Local Session
Source Ports       :
    Both           :Fa0/2
Destination Ports :Fa0/3
    Encapsulation :Replicate
          Ingress:Enabled, default VLAN = 5
    Ingress encapsulation:DOT1Q

Session 2
---------
Type               :Local Session
Source Ports       :
    Both           :Fa0/1
Destination Ports :Fa0/4
    Encapsulation :Replicate
          Ingress:Enabled
    Ingress encapsulation:DOT1Q
```

## Related Commands

| Command | Description |
|---|---|
| monitor session | Starts or modifies a SPAN or RSPAN session. |

# show mvr

Use the **show mvr** privileged EXEC command without keywords to display the current Multicast VLAN Registration (MVR) global parameter values, including whether or not MVR is enabled, the MVR multicast VLAN, the maximum query response time, the number of multicast groups, and the MVR mode (dynamic or compatible).

**show mvr** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mvr** command:

```
Switch# show mvr
MVR Running: TRUE
MVR multicast VLAN: 1
MVR Max Multicast Groups: 256
MVR Current multicast groups: 0
MVR Global query response time: 5 (tenths of sec)
MVR Mode: compatible
```

In the preceding display, the maximum number of multicast groups is fixed at 256. The MVR mode is either compatible (for interoperability with Catalyst 2900 XL and Catalyst 3500 XL switches) or dynamic (where operation is consistent with IGMP snooping operation and dynamic MVR membership on source ports is supported).

**Related Commands**

| Command | Description |
|---|---|
| **mvr (global configuration)** | Enables and configures multicast VLAN registration on the switch. |
| **mvr (interface configuration)** | Configures MVR ports. |
| **show mvr interface** | Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **interface** and **members** keywords are appended to the command. |
| **show mvr members** | Displays all ports that are members of an MVR multicast group or, if there are no members, means the group is inactive. |

# show mvr interface

Use the **show mvr interface** privileged EXEC command without keywords to display the Multicast VLAN Registration (MVR) receiver and source ports. Use the command with keywords to display MVR parameters for a specific receiver port.

**show mvr interface** [*interface-id* [**members** [**vlan** *vlan-id*]]] [ **|** {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) Display MVR type, status, and Immediate Leave setting for the interface.<br>Valid interfaces include physical ports (including type, module, and port number. |
| **members** | (Optional) Display all MVR groups to which the specified interface belongs. |
| **vlan** *vlan-id* | (Optional) Display all MVR group members on this VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(35)SE | The Mode and VLAN fields were added to the output display. |

## Usage Guidelines

If the entered port identification is a non-MVR port or a source port, the command returns an error message. For receiver ports, it displays the port type, per port status, and Immediate-Leave setting.

If you enter the **show mvr interface** *interface-id* command and the specified port is a non-MVR port, the output displays NON MVR in the Type field. For active MVR ports, it displays the port type (RECEIVER or SOURCE), mode (access or trunk), VLAN, status, and Immediate-Leave setting.

If you enter the **members** keyword, all MVR group members on the interface appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mvr interface** command:

```
Switch# show mvr interface
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/1   Receiver        Trunk           1       ACTIVE/UP       DISABLED
Fa0/1   Receiver        Trunk           2000    ACTIVE/DOWN     DISABLED
Fa0/2   Receiver        Trunk           2       ACTIVE/UP       DISABLED
Fa0/2   Receiver        Trunk           3000    ACTIVE/UP       DISABLED
Fa0/3   Receiver        Trunk           2       ACTIVE/UP       DISABLED
Fa0/3   Receiver        Trunk           3000    ACTIVE/UP       DISABLED
Fa0/10  Source          Access          10      ACTIVE/UP       DISABLED
```

In the preceding display, Status is defined as follows:

- Active means the port is part of a VLAN.
- Up/Down means that the port is forwarding/nonforwarding.
- Inactive means that the port is not yet part of any VLAN.

This is an example of output from the **show mvr interface fastethernet0/10** command:

```
switch# show mvr interface fa0/10
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/10  RECEIVER        Trunk           201     ACTIVE/DOWN     DISABLED
```

This is an example of output from the **show mvr interface fastethernet0/1** command. In this example, the port is not an MVR member:

```
switch# show mvr interface fa0/1
Port    Type            Mode            VLAN    Status          Immediate Leave
----    ----            ----            ----    -------         ---------------
Fa0/1   NON MVR         Access          0       INACTIVE        DISABLED
```

This is an example of output from the **show mvr interface gigabitethernet0/1 members** command:

```
Switch# show mvr interface gigabitethernet0/1 members
239.255.0.0     vlan 202     DYNAMIC ACTIVE
239.255.0.1     vlan 202     DYNAMIC ACTIVE
239.255.0.2     vlan 202     DYNAMIC ACTIVE
239.255.0.3     vlan 203     DYNAMIC ACTIVE
239.255.0.4     vlan 203     DYNAMIC ACTIVE
239.255.0.5     vlan 203     DYNAMIC ACTIVE
```

## Related Commands

| Command | Description |
|---|---|
| **mvr (global configuration)** | Enables and configures multicast VLAN registration on the switch. |
| **mvr (interface configuration)** | Configures MVR ports. |
| **show mvr** | Displays the global MVR configuration on the switch. |
| **show mvr members** | Displays all receiver ports that are members of an MVR multicast group. |

# show mvr members

Use the **show mvr members** privileged EXEC command to display all receiver and source ports that are currently members of an IP multicast group.

**show mvr members** [*ip-address*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *ip-address* | (Optional) The IP multicast address. If the address is entered, all receiver and source ports that are members of the multicast group appear. If no address is entered, all members of all Multicast VLAN Registration (MVR) groups are listed. If a group has no members, the group is listed as Inactive. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(35)SE | The VLAN and Membership fields were added to the output display. |

## Usage Guidelines

The **show mvr members** command applies to receiver and source ports. For MVR-compatible mode, all source ports are members of all multicast groups.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show mvr members** command:

```
Switch# show mvr members
MVR Group     Status   Members  VLAN   Membership
------------  ------   -------  ----   ----------
239.1.1.1     ACTIVE   Fa0/1    1      Static
239.1.1.1     ACTIVE   Fa0/1    2000   Static
239.1.1.1     ACTIVE   Fa0/2    2      Static
239.1.1.1     ACTIVE   Fa0/2    3000   Static
239.1.1.2     ACTIVE   Fa0/1    1      Static
239.1.1.2     ACTIVE   Fa0/2    2      Static

<output truncated>
```

This is an example of output from the **show mvr members 239.255.0.2** command. It shows how to view the members of the IP multicast group 239.255.0.2:

```
Switch# show mvr members 239.255.0.2
239.255.0.2     ACTIVE          Gi0/1(d), Gi0/2(d), Gi0/3(d),
                                Gi0/4(d), Gi0/5(s)
```

## Related Commands

| Command | Description |
|---|---|
| **mvr (global configuration)** | Enables and configures multicast VLAN registration on the switch. |
| **mvr (interface configuration)** | Configures MVR ports. |
| **show mvr** | Displays the global MVR configuration on the switch. |
| **show mvr interface** | Displays the configured MVR interfaces, status of the specified interface, or all multicast groups to which the interface belongs when the **members** keyword is appended to the command. |

# show pagp

Use the **show pagp** user EXEC command to display Port Aggregation Protocol (PAgP) channel-group information.

**show pagp** [*channel-group-number*] {**counters** | **internal** | **neighbor**} [ | {**begin** | **exclude** | **include**} *expression*]]

**Note** PAgP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| *channel-group*-number | (Optional) Number of the channel group. The range is 1 to 48. |
| **counters** | Display traffic information. |
| **internal** | Display internal information. |
| **neighbor** | Display neighbor information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can enter any **show pagp** command to display the active channel-group information. To display the nonactive information, enter the **show pagp** command with a channel-group number.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* are appear.

## Examples

This is an example of output from the **show pagp 1 counters** command:

```
Switch> show pagp 1 counters
             Information         Flush
Port         Sent   Recv     Sent   Recv
---------------------------------------
Channel group: 1
  Gi0/1      45     42       0      0
  Gi0/2      45     41       0      0
```

This is an example of output from the **show pagp 1 internal** command:

```
Switch> show pagp 1 internal
Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
        A - Device is in Auto mode.
Timers: H - Hello timer is running.        Q - Quit timer is running.
        S - Switching timer is running.    I - Interface timer is running.

Channel group 1
                                Hello    Partner  PAgP     Learning  Group
Port        Flags State   Timers  Interval Count   Priority   Method  Ifindex
Gi0/1       SC    U6/S7   H       30s      1        128        Any      16
Gi0/2       SC    U6/S7   H       30s      1        128        Any      16
```

This is an example of output from the **show pagp 1 neighbor** command:

```
Switch> show pagp 1 neighbor
   Flags:  S - Device is sending Slow hello.  C - Device is in Consistent state.
           A - Device is in Auto mode.        P - Device learns on physical port.

   Channel group 1 neighbors
               Partner              Partner          Partner           Partner Group
   Port        Name                 Device ID        Port         Age  Flags   Cap.
   Gi0/1       switch-p2            0002.4b29.4600   Gi0/1          9s SC      10001
   Gi0/2       switch-p2            0002.4b29.4600   Gi0/2         24s SC      10001
```

## Related Commands

| Command | Description |
|---|---|
| clear pagp | Clears PAgP channel-group information. |

# show parser macro

Use the **show parser macro** user EXEC command to display the parameters for all configured macros or for one macro on the switch.

**show parser macro** [{**brief** | **description** [**interface** *interface-id*] | **name** *macro-name*}] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **brief** | (Optional) Display the name of each macro. |
| **description** [**interface** *interface-id*] | (Optional) Display all macro descriptions or the description of a specific interface. |
| **name** *macro-name* | (Optional) Display information about a single macro identified by the macro name. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is a partial output example from the **show parser macro** command:

```
Switch# show parser macro
Total number of macros = 2
------------------------------------------------------------------
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
------------------------------------------------------------------
Macro name : test1
Macro type : customizable
no shutdown
flowcontrol receive on
speed 100
------------------------------------------------------------------
```

This is an example of output from the **show parser macro name** command:

```
Switch# show parser macro name sample-macro1
Macro name : sample-macro1
Macro type : customizable
duplex full
speed auto
mdix auto
```

This is an example of output from the **show parser macro brief** command:

```
Switch# show parser macro brief
    customizable     : sample-macro1
    customizable     : test1
```

## Related Commands

| Command | Description |
|---|---|
| **macro apply** | Applies a macro on an interface or applies and traces a macro on an interface. |
| **macro description** | Adds a description about the macros that are applied to an interface. |
| **macro global** | Applies a macro on a switch or applies and traces a macro on a switch. |
| **macro global description** | Adds a description about the macros that are applied to the switch. |
| **macro name** | Creates a macro. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# show policer aggregate

Use the **show policer aggregate** user EXEC command to display quality of service (QoS) aggregate policer information for all aggregate policers or a specific policer.

**show policer aggregate** [*aggregate-policer-name*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *aggregate-policer-name* | (Optional) The name of the aggregate policer. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show policer aggregate** command:

```
Switch> show policer aggregate my-policer
aggregate-policer: my-policer

     police cir 12000000 bc 5000
       conform-action transmit
       exceed-action set-cos-transmit cos table 67577

In use by policymap: pin
```

## Related Commands

| Command | Description |
|---|---|
| **police aggregate (policy-map class configuration)** | Applies an aggregate policer to multiple classes in the same policy map. |
| **policer aggregate (global configuration)** | Creates an aggregate policer to police all traffic received on an interface. |

# show policer cpu uni-eni

Use the **show policer cpu uni-eni** user EXEC command to display control-plane policer information for the user network interfaces (UNIs) and enhanced network interfaces (ENIs) on the switch, including frames dropped or the configured threshold rate for the control-plane security feature on the switch.

**show policer cpu uni-eni** [**drop** [*policer-number*] | **rate**] [**interface** *interface-id*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **drop** | (Optional) Display control-plane frame-drop count for the specified policer number or for all control-plane policers (0 to 26). |
| **policer** *number* | (Optional) Display drop statistics for a specific user network interface (UNI) or enhanced network interface (ENI) policer number. The range is from 0 to 26. |
| **rate** | (Optional) Display the configured threshold rate for CPU policers. |
| **interface** *interface-id* | Optional) Display the control-plane information for the specified physical interface. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG1 | Outputs for the **show policer cup uni drop** changed. |
| 12.2(44)SE | The **show policer cpu uni** command was changed to the **show policer cpu uni-eni** command. |

## Usage Guidelines

This command displays policer information that applies to UNIs and ENIs on the switch. Rate-limiting and policers are the same on both port types, except on ENIs on which a Layer 2 control protocol (CDP, STP, LLDP, LACP, or PAgP) has been enabled.

The **show policer cpu uni-eni drop** privileged EXEC command displays the number of accepted and dropped frames for all policers on the switch or for the specified policer number.

The **show policer cpu uni-eni rate** command displays the CPU protection rate-limit threshold on the switch that was configured by entering the **policer cpu uni** *rate* global configuration command or the default rate of 16000 bits per second (bps).

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show policer cpu uni-eni drop** command. Note that CPU protection only uses policers 0 to 26.

```
Switch# show policer cpu uni-eni drop
=======================================
Port                  In           Dropped
Name                Frames          Frames
Fa0/1                300              0
Fa0/2                  0              0
Fa0/3                  0              0
Fa0/4                  0              0
Fa0/5                200              0
Fa0/6                  0              0
Fa0/7                  0              0
Fa0/8                  0              0
Fa0/9             508055         325086
Fa0/10                 0              0
Fa0/11                 0              0
Fa0/12                 0              0
Fa0/13                 0              0
Fa0/14                 0              0
Fa0/15                 0              0
Fa0/16                 0              0
Fa0/17                 0              0
Fa0/18                 0              0
Fa0/19                 0              0
Fa0/20                 0              0
Fa0/21                 0              0
Fa0/22                 0              0
Fa0/23                 0              0
Fa0/24                 0              0
Gi0/1                  0              0
Gi0/2                  0              0
drop-all               0        1849645
```

This is an example of the new output format for the **show policer cpu uni-eni drop interface** command:

```
Switch# show policer cpu uni-eni drop interface gigabitethernet 0/1
============================
Policer assigned for Gi0/2
============================
Protocols using this policer:
"VTP" "CISCO_L2" "KEEPALIVE" "SWITCH_IGMP" "SWITCH_L2PT"
Policer rate: 160000 bps
In frames: 48014
Drop frames: 28630
```

This is an example of output from the **show policer cpu uni-eni rate** command when the default rate is used.

```
Switch> show policer cpu uni-eni rate
CPU UNI/ENI port police rate = 160000 bps
```

## Related Commands

| Command | Description |
|---|---|
| **policer cpu uni** | Configures a CPU policer threshold rate for the switch. |
| **show platform policer cpu** | Displays allocated policer indexes and the corresponding features for all ports or the specified port. |

# show policy-map

Use the **show policy-map** user EXEC command to display quality of service (QoS) policy maps, which define classification criteria for incoming and outgoing traffic and the actions to be performed on the classified traffic.

**show policy-map** [*policy-map-name* | **interface** [*interface-id*] [**input** | **output**] [**class** *class-name*]] [ | {begin | exclude | include} expression]

## Syntax Description

| | |
|---|---|
| *policy-map-name* | (Optional) Display the specified policy-map name. |
| **class** *class-map-name* | (Optional) Display QoS policy actions for an individual class. |
| **interface** [*interface-id*] [**input** \| **output**] | (Optional) Display information and statistics about policy maps applied to all ports or the specified port. If you specify a port, you can specify additional keywords.The keywords have these meanings:<br>• *interface-id*—Display information about policy maps on the specified physical interface.<br>• **input**—Display information about input policy maps on the switch or applied to the specified port.<br>• **output**—Display the information about output policy-maps on the switch or applied to the specified port. |
| **class** *class-name* | (Optional) Display policy-map statistics for an individual class. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show policy-map** command:

```
Switch> show policy-map
Policy Map videowizard_policy2
  class  videowizard_10-10-10-10
police 100000000 2000000 exceed-action drop

 Policy Map mypolicy
  class  dscp5
```

This is an example of output from the **show policy-map** command for a specific policy map:

```
Switch> show policy-map top2
  Policy Map top2
    Class class-default
      shape average 11111124
      service-policy pout
```

This is an example of output from the **show policy-map** command for an output policy map:

```
Switch> show policy-map pout
  Policy Map pout
    Class ip1
      priority
     police cir percent 10
       conform-action transmit
       exceed-action drop
      queue-limit 250
      queue-limit precedence  1 100
    Class ip2
      Average Rate Traffic Shaping
      cir 5%
    Class ip3
      bandwidth percent 10
      queue-limit 200
      queue-limit precedence  3 100
```

This is an example of output from the **show policy-map** command for an input policy map:

```
Switch> show policy-map pin-police
Policy Map pin-police
    Class ip1
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
```

This is an example of output from the **show policy-map interface** command for an interface with a two-level output policy map applied:

```
Switch> show policy-map interface fastethernet0/3
 FastEthernet0/3

  Service-policy output: top2

    Class-map: class-default (match-any)
      209871 packets
      Match: any
        56 packets
      Traffic Shaping
        Average Rate Traffic Shaping
        CIR 11111124 (bps)
      Output Queue:
        Tail Packets Drop: 195421

      Service-policy : pout

        Class-map: ip1 (match-all)
          9309 packets
          Match: ip precedence 1
          Priority
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
      conform: 4916 (packets) exceed: 4393 (packets)
```

```
      Queue Limit
        queue-limit 250 (packets)
        queue-limit precedence  1 100 (packets)
      Output Queue:
        Max Tail Drop Threshold: 250
        Tail Packets Drop: 4393

    Class-map: ip2 (match-all)
      0 packets
      Match: ip precedence 2
      Traffic Shaping
        Average Rate Traffic Shaping
        CIR 5%       555555 (bps)
      Output Queue:
        Max Tail Drop Threshold: 48
        Tail Packets Drop: 0

    Class-map: ip3 (match-all)
      0 packets
      Match: ip precedence 3
      Bandwidth percent 10         1111110 (bps)
      Queue Limit
        queue-limit 200 (packets)
        queue-limit precedence  3 100 (packets)
      Output Queue:
        Max Tail Drop Threshold: 200
        Tail Packets Drop: 0

    Class-map: class-default (match-any)
      200562 packets
      Match: any
        56 packets
      Output Queue:
        Tail Packets Drop: 191028
```

This is an example of output from the **show policy-map interface** command for an interface with an input policy applied:

```
Switch> show policy-map interface gigabitethernet0/1
 GigabitEthernet0/1

  Service-policy input: pin-police

    Class-map: ip1 (match-all)
      0 packets
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: ip precedence 1
     police cir 20000000 bc 625000
       conform-action transmit
       exceed-action drop
      conform: 27927 (packets) exceed: 272073 (packets)

    Class-map: class-default (match-any)
      0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: any
        0 packets
        5 minute rate 0 bps
```

Table 2-15 describes the fields in the **show policy-map interface** display. The fields in the table are grouped according to the relevant QoS feature.

***Table 2-15 show policy-map interface Field Descriptions***

| Field | Description |
|---|---|
| **Fields associated with classes or service policies** | |
| Service-policy input/output | Name of the input or output service policy applied to the specified interface. |
| Class-map | Class of traffic shown. Output appears for each configured class in the policy. The choice for implementing class matches (match-all or match-any) might also appear next to the traffic class. |
| packets | Number of packets identified as belonging to the traffic class. |
| Match | Match criteria specified for the class of traffic. This includes criteria such as class of service (CoS) value, IP precedence value, Differentiated Services Code Point (DSCP) value, access groups, and QoS groups. |
| **Fields associated with policing** | |
| police | Shown when the **police** command has been configured to enable traffic policing. Displays the specified committed information rate (CIR) and conform burst size (BC) used for policing packets. |
| conform-action | Displays the action to be taken on packets marked as conforming to a specified rate. |
| conform | Displays the number of packets marked as conforming to the specified rate. |
| exceed-action | Displays the actions to be taken on packets marked as exceeding a specified rate. |
| exceed | Displays the number of packets marked as exceeding the specified rate. |
| **Fields associated with queuing** | |
| Queue Limit | Queue size configured for the class in number of packets. |
| Output Queue | The queue created for this class of traffic. |
| Tail packets dropped | The number of packets dropped when the mean queue depth is greater than the maximum threshold value. |
| **Fields associated with traffic scheduling** | |
| Traffic shaping | The rate used for shaping traffic. |
| Bandwidth | Bandwidth configured for this class in kbps or a percentage. |
| Priority | Indicates that this class is configured for priority queuing. |

## Related Commands

| Command | Description |
|---|---|
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |

# show port-security

Use the **show port-security** privileged EXEC command to display port-security settings for an interface or for the switch.

**show port-security** [**interface** *interface-id*] [**address** | **vlan**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Display port security settings for the specified interface. Valid interfaces include physical ports (including type, module, and port number). |
| **address** | (Optional) Display all secure MAC addresses on all ports or a specified port. |
| **vlan** | (Optional) Display port security settings for all VLANs on the specified interface. This keyword is visible only on interfaces that have the switchport mode set to **trunk**. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you enter the command without keywords, the output includes the administrative and operational status of all secure ports on the switch.

If you enter an *interface-id*, the command displays port security settings for the interface.

If you enter the **address** keyword, the command displays the secure MAC addresses for all interfaces and the aging information for each secure address.

If you enter an *interface-id* and the **address** keyword, the command displays all the MAC addresses for the interface with aging information for each secure address. You can also use this command to display all the MAC addresses for an interface even if you have not enabled port security on it.

If you enter the **vlan** keyword, the command displays the configured maximum and the current number of secure MAC addresses for all VLANs on the interface. This option is visible only on interfaces that have the switchport mode set to **trunk**.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of the output from the **show port-security** command:

```
Switch# show port-security
Secure Port      MaxSecureAddr  CurrentAddr  SecurityViolation  Security Action
                    (Count)        (Count)      (Count)
---------------------------------------------------------------------------
     Gi0/1         1               0             0             Shutdown
---------------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface** *interface-id* command:

```
Switch# show port-security interface gigabitethernet0/1
Port Security : Enabled
Port status : SecureUp
Violation mode : Shutdown
Maximum MAC Addresses : 1
Total MAC Addresses : 0
Configured MAC Addresses : 0
Aging time : 0 mins
Aging type : Absolute
SecureStatic address aging : Disabled
Security Violation count : 0
```

This is an example of output from the **show port-security address** command:

```
Switch# show port-security address
Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi0/2       1
------------------------------------------------------------------
Total Addresses in System (excluding one mac per port)     : 1
Max Addresses limit in System (excluding one mac per port) : 6272
```

This is an example of output from the **show port-security interface gigabitethernet0/2 address** command:

```
Switch# show port-security interface gigabitethernet0/2 address
          Secure Mac Address Table
------------------------------------------------------------------
Vlan    Mac Address       Type                Ports   Remaining Age
                                                         (mins)
----    -----------       ----                -----   -------------
   1    0006.0700.0800    SecureConfigured    Gi0/2       1
------------------------------------------------------------------
Total Addresses: 1
```

This is an example of output from the **show port-security interface** *interface-id* **vlan** command:

```
Switch# show port-security interface gigabitethernet0/2 vlan
Default maximum:not set, using 5120
VLAN  Maximum    Current
    5    default          1
   10    default         54
   11    default        101
   12    default        101
   13    default        201
   14    default        501
```

**Related Commands**

| Command | Description |
|---|---|
| clear port-security | Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface. |
| switchport port-security | Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses. |

# show port-type

Use the **show port-type** privileged EXEC command to display interface type information for the Cisco ME switch.

**show port-type** [**eni** | **nni** | **uni**] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **eni** | Enhanced network interface. |
| **nni** | Network node interface. |
| **uni** | User network interface. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(44)SE | The **eni** keyword was added. |

## Usage Guidelines

If you enter the command without keywords, the output includes the interface type information for all ports on the switch. If you specify the port type (**eni**, **nni**, or **uni**), the output includes information for the specified port type.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show port-type** command with no keywords:

```
Switch# show port-type
Port      Name               Vlan       Port Type
--------- ------------------ ---------- ----------------------------
Fa0/1                        1          User Network Interface (uni)
Fa0/2                        1          User Network Interface (uni)
Fa0/3                        1          User Network Interface (uni)
Fa0/4                        1          User Network Interface (uni)
Fa0/5                        1          User Network Interface (uni)
Fa0/6                        1          User Network Interface (uni)
Fa0/7                        1          User Network Interface (uni)
Fa0/8                        1          User Network Interface (uni)
Fa0/9                        1          User Network Interface (uni)
Fa0/10                       1          User Network Interface (uni)
Fa0/11                       1          User Network Interface (uni)
Fa0/12                       1          User Network Interface (uni)
Fa0/13                       1          User Network Interface (uni)
```

```
Fa0/14                       1          User Network Interface (uni)
Fa0/15                       1          User Network Interface (uni)
Fa0/16                       1          User Network Interface (uni)
Fa0/17                       routed     User Network Interface (uni)
Fa0/18                       1          User Network Interface (uni)
Fa0/19                       1          User Network Interface (uni)
Fa0/20                       1          User Network Interface (uni)
Fa0/21                       1          User Network Interface (uni)
Fa0/22                       1          User Network Interface (uni)
Fa0/23                       10         User Network Interface (uni)
Fa0/24                       10         User Network Interface (uni)
Gi0/1                        1          Network Node Interface (nni)
Gi0/2                        1          Network Node Interface (nni)
```

This is an example of output from the **show port-type** command using keywords:

```
Switch# show port-type nni | exclude Gigabitethernet0/1
Port      Name                Vlan       Port Type
--------- ------------------- ---------- ----------------------------
Gi0/2                         1          Network Node Interface (nni)
```

## Related Commands

| Command | Description |
|---|---|
| port-type | Changes the interface type for a specific port. |

# show sdm prefer

Use the **show sdm prefer** privileged EXEC command to display the Switch Database Management (SDM) template used to allocate system resources.

**show sdm prefer** [**layer-2**] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **layer-2** | (Optional) Display resource allocations for the template that supports Layer 2 features and does not support routing. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The numbers displayedrepresent an approximate maximum number for each feature resource. The actual number might vary, depending on the actual number of other features configured.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show sdm prefer** command, displaying the template in use:

```
Switch# show sdm prefer
The current template is ''layer-2'' template.
The selected template optimizes the resources in
the switch to support this level of features for
8 routed interfaces and 1024 VLANs.

  number of unicast mac addresses:                 2K
  number of IPv4 IGMP groups:                      1K
  number of IPv4 multicast routes:                 0
  number of unicast IPv4 routes:                   0
  number of IPv4 policy based routing aces:        0
  number of IPv4/MAC qos aces:                     512
  number of IPv4/MAC security aces:                1K
```

# show spanning-tree

Use the **show spanning-tree** user EXEC command to display spanning-tree state information.

**show spanning-tree** [*bridge-group* | **active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **mst** | **pathcost method** | **root** | **summary** [**totals**] | **vlan** *vlan-id*] [ | {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree** *bridge-group* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [| {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree vlan** *vlan-id* [**active** [**detail**] | **blockedports** | **bridge** | **detail** [**active**] | **inconsistentports** | **interface** *interface-id* | **root** | **summary**] [ | {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree** {**vlan** *vlan-id* | *bridge-group*} **bridge** [**address** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **priority** [**system-id**] | **protocol**] [ | {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree** {**vlan** *vlan-id* | *bridge-group*} **root** [**address** | **cost** | **detail** | **forward-time** | **hello-time** | **id** | **max-age** | **port** | **priority** [**system-id**] [ | {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree interface** *interface-id* [**active** [**detail**] | **cost** | **detail** [**active**] | **inconsistency** | **portfast** | **priority** | **rootcost** | **state**] [ | {**begin** | **exclude** | **include**} *expression*]

**show spanning-tree mst** [**configuration [digest**]] | [*instance-id* [**detail** | **interface** *interface-id* [**detail**]] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *bridge-group* | (Optional) Specify the bridge group number. The range is 1 to 255. |
| **active** [**detail**] | (Optional) Display spanning-tree information only on active interfaces (available only in privileged EXEC mode). |
| **blockedports** | (Optional) Display blocked port information (available only in privileged EXEC mode). |
| **bridge** [**address** \| **detail** \| **forward-time** \| **hello-time** \| **id** \| **max-age** \| **priority** [**system-id**] \| **protocol**] | (Optional) Display status and configuration of this switch (optional keywords available only in privileged EXEC mode). |
| **detail** [**active**] | (Optional) Display a detailed summary of interface information (**active** keyword available only in privileged EXEC mode). |
| **inconsistentports** | (Optional) Display inconsistent port information (available only in privileged EXEC mode). |

| | |
|---|---|
| **interface** *interface-id* [**active** [**detail**] \| **cost** \| **detail** [**active**] \| **inconsistency** \| **portfast** \| **priority** \| **rootcost** \| **state**] | (Optional) Display spanning-tree information for the specified interface (all options except **portfast** and **state** available only in privileged EXEC mode). Enter each interface separated by a space. Ranges are not supported. Valid interfaces include physical network node interfaces (NNIs), enhanced network interfaces (ENIs), VLANs, and NNI or ENI port channels. The VLAN range is 1 to 4094. The port-channel range is 1 to 48.<br>**Note** Spanning Tree Protocol (STP) is not supported on user node interfaces (UNIs). If you enter a UNI interface ID, no spanning-tree information is displayed. |
| **mst** [**configuration** [**digest**]] [*instance-id* [**detail** \| **interface** *interface-id* [**detail**]] | (Optional) Display the multiple spanning-tree (MST) region configuration and status (available only in privileged EXEC mode).<br>The keywords have these meanings:<br>• **digest**—(Optional) Display the MD5 digest included in the current MST configuration identifier (MSTCI). Two separate digests, one for standard and one for prestandard switches, appear (available only in privileged EXEC mode).<br>The terminology was updated for the implementation of the IEEE standard, and the *txholdcoun*t field was added.<br>The new master role appears for boundary ports.<br>The word *pre-standard* or *Pre-STD* appears when an IEEE standard bridge sends prestandard BPDUs on a port.<br>The word *pre-standard (config)* or *Pre-STD-Cf* appears when a port has been configured to send prestandard BPDUs and no prestandard BPDU has been received on that port.<br>The word *pre-standard (rcvd)* or *Pre-STD-Rx* appears when a prestandard BPDU has been received on a port that has not been configured to send prestandard BPDUs.<br>A *dispute* flag appears when a designated port receives inferior designated information until the port returns to the forwarding state or ceases to be designated.<br>• *instance-id*—You can specify a single instance ID, a range of IDs separated by a hyphen, or a series of IDs separated by a comma. The range is 1 to 4094. The display shows the number of currently configured instances.<br>• **interface** *interface-id*—(Optional) Valid interfaces include VLANs, physical NNIs and NNI port channels, and physical ENIs and ENI port channels. STP is not supported on UNIs.<br>The VLAN range is 1 to 4094. The port-channel range is 1 to 48.<br>• **detail**—(Optional) Display detailed information for the instance or interface. |
| **pathcost method** | (Optional) Display the default path cost method (available only in privileged EXEC mode). |
| **root** [**address** \| **cost** \| **detail** \| **forward-time** \| **hello-time** \| **id** \| **max-age** \| **port** \| **priority** [**system-id**]] | (Optional) Display root switch status and configuration (all keywords available only in privileged EXEC mode). |

| | |
|---|---|
| **summary** [**totals**] | (Optional) Display a summary of port states or the total lines of the spanning-tree state section. |
| **vlan** *vlan-id* [**active** [**detail**] \| **backbonefast** \| **blockedports** \| **bridge** [**address** \| **detail** \| **forward-time** \| **hello-time** \| **id** \| **max-age** \| **priority** [**system-id**] \| **protocol**] | (Optional) Display spanning-tree information for the specified VLAN (some keywords available only in privileged EXEC mode). You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The **digest** keyword was added, and new digest and transmit hold count fields appear. |

## Usage Guidelines

STP is not supported on UNIs. Valid spanning-tree information is available only for NNIs or ENIs.

If the *vlan-id* variable is omitted, the command applies to the spanning-tree instance for all VLANs.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show spanning-tree active** command:

```
Switch# show spanning-tree active
VLAN0001
  Spanning tree enabled protocol ieee
  Root ID    Priority    32768
             Address     0001.42e2.cdd0
             Cost        3038
             Port        24 (GigabitEthernet0/1)
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec

  Bridge ID  Priority    49153  (priority 49152 sys-id-ext 1)
             Address     0003.fd63.9580
             Hello Time   2 sec  Max Age 20 sec  Forward Delay 15 sec
             Aging Time 300
  Uplinkfast enabled

Interface        Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
Gi0/1            Root FWD 3019      128.24   P2p
<output truncated>
```

This is an example of output from the **show spanning-tree detail** command:

```
Switch# show spanning-tree detail
VLAN0001 is executing the ieee compatible Spanning Tree protocol
  Bridge Identifier has priority 49152, sysid 1, address 0003.fd63.9580
  Configured hello time 2, max age 20, forward delay 15
  Current root has priority 32768, address 0001.42e2.cdd0
  Root port is 24 (GigabitEthernet0/1), cost of root path is 3038
  Topology change flag not set, detected flag not set
  Number of topology changes 0 last change occurred 1d16h ago
  Times:  hold 1, topology change 35, notification 2
          hello 2, max age 20, forward delay 15
  Timers: hello 0, topology change 0, notification 0, aging 300
  Uplinkfast enabled

 Port 1 (GigabitEthernet0/1) of VLAN0001 is forwarding
   Port path cost 3019, Port priority 128, Port Identifier 128.24.
   Designated root has priority 32768, address 0001.42e2.cdd0
   Designated bridge has priority 32768, address 00d0.bbf5.c680
   Designated port id is 128.25, designated path cost 19
   Timers: message age 2, forward delay 0, hold 0
   Number of transitions to forwarding state: 1
   Link type is point-to-point by default
   BPDU: sent 0, received 72364
<output truncated>
```

This is an example of output from the **show spanning-tree interface** *interface-id* command:

```
Switch# show spanning-tree interface gigabitethernet0/1
Vlan             Role Sts Cost      Prio.Nbr Type
---------------- ---- --- --------- -------- --------------------------------
VLAN0001         Root FWD 3019      128.24   P2p
```

This is an example of output from the **show spanning-tree summary** command:

```
Switch# show spanning-tree summary
Switch is in pvst mode
Root bridge for: none
EtherChannel misconfiguration guard is enabled
Extended system ID   is enabled
Portfast             is disabled by default
PortFast BPDU Guard  is disabled by default
Portfast BPDU Filter is disabled by default
Loopguard            is disabled by default
Pathcost method used is short

Name                   Blocking Listening Learning Forwarding STP Active
---------------------- -------- --------- -------- ---------- ----------
VLAN0001                  1        0         0        11         12
VLAN0002                  3        0         0        1          4
VLAN0004                  3        0         0        1          4
VLAN0006                  3        0         0        1          4
VLAN0031                  3        0         0        1          4
VLAN0032                  3        0         0        1          4
<output truncated>
---------------------- -------- --------- -------- ---------- ----------
37 vlans                  109      0         0        47         156
Station update rate set to 150 packets/sec.
```

This is an example of output from the **show spanning-tree mst configuration** command:

```
Switch# show spanning-tree mst configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  ------------------
0         1-9,21-4094
1         10-20
----------------------------
```

This is an example of output from the **show spanning-tree mst configuration digest** command:

```
Switch# show spanning-tree mst configuration
% Switch is not in mst mode
Name      []
Revision  0     Instances configured 1
Digest          0xAC36177F50283CD4B83821D8AB26DE62
Pre-std Digest  0xBB3B6C15EF8D089BB55ED10D24DF44DE
```

This is an example of output from the **show spanning-tree mst interface** *interface-id* command:

```
Switch# show spanning-tree mst interface gigabitethernet0/1
GigabitEthernet0/1 of MST00 is root forwarding
Edge port: no             (default)        port guard : none        (default)
Link type: point-to-point (auto)           bpdu filter: disable     (default)
Boundary : boundary       (STP)            bpdu guard : disable     (default)
Bpdus sent 5, received 74

Instance role state cost      prio vlans mapped
0        root FWD   200000    128  1,12,14-4094
```

This is an example of output from the **show spanning-tree mst 0** command:

```
Switch# show spanning-tree mst 0
###### MST00        vlans mapped: 1-9,21-4094
Bridge      address 0002.4b29.7a00  priority  32768 (32768 sysid 0)
Root        address 0001.4297.e000  priority  32768 (32768 sysid 0)
                    port    Gi0/1           path cost 200038
IST master *this switch
Operational hello time 2, forward delay 15, max age 20, max hops 20
Configured  hello time 2, forward delay 15, max age 20, max hops 20

Interface              role state cost      prio type
--------------------   ---- ----- --------- ---- --------------------------------
GigabitEthernet0/1     root FWD   200000    128  P2P bound(STP)
GigabitEthernet0/2     desg FWD   200000    128  P2P bound(STP)
Port-channel1          desg FWD   200000    128  P2P bound(STP)
```

## Related Commands

| Command | Description |
|---|---|
| clear spanning-tree counters | Clears the spanning-tree counters. |
| clear spanning-tree detected-protocols | Restarts the protocol migration process. |
| spanning-tree bpdufilter | Prevents an interface from sending or receiving bridge protocol data units (BPDUs). |
| spanning-tree bpduguard | Puts an interface in the error-disabled state when it receives a BPDU. |
| spanning-tree cost | Sets the path cost for spanning-tree calculations. |
| spanning-tree extend system-id | Enables the extended system ID feature. |
| spanning-tree guard | Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface. |
| spanning-tree link-type | Overrides the default link-type setting for rapid spanning-tree transitions to the forwarding state. |
| spanning-tree loopguard default | Prevents alternate or root ports from becoming the designated port because of a failure that leads to a unidirectional link. |
| spanning-tree mst configuration | Enters multiple spanning-tree (MST) configuration mode through which the MST region configuration occurs. |
| spanning-tree mst cost | Sets the path cost for MST calculations. |
| spanning-tree mst forward-time | Sets the forward-delay time for all MST instances. |
| spanning-tree mst hello-time | Sets the interval between hello BPDUs sent by root switch configuration messages. |
| spanning-tree mst max-age | Sets the interval between messages that the spanning tree receives from the root switch. |
| spanning-tree mst max-hops | Sets the number of hops in an MST region before the BPDU is discarded and the information held for an interface is aged. |
| spanning-tree mst port-priority | Configures an interface priority. |
| spanning-tree mst priority | Configures the switch priority for the specified spanning-tree instance. |
| spanning-tree mst root | Configures the MST root switch priority and timers based on the network diameter. |
| spanning-tree port-priority | Configures an interface priority. |
| spanning-tree portfast (global configuration) | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled interfaces or enables the Port Fast feature on all nontrunking interfaces. |
| spanning-tree portfast (interface configuration) | Enables the Port Fast feature on an interface and all its associated VLANs. |
| spanning-tree vlan | Configures spanning tree on a per-VLAN basis. |

# show storm-control

Use the **show storm-control** user EXEC command to display broadcast, multicast, or unicast storm control settings on the switch or on the specified interface or to display storm-control history.

**show storm-control** [*interface-id*] [**broadcast | multicast | unicast**] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) Interface ID for the physical port (including type, module, and port number). |
| **broadcast** | (Optional) Display broadcast storm threshold setting. |
| **multicast** | (Optional) Display multicast storm threshold setting. |
| **unicast** | (Optional) Display unicast storm threshold setting. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you enter an *interface-id*, the storm control thresholds appear for the specified interface.

If you do not enter an *interface-id*, settings appear for one traffic type for all ports on the switch.

If you do not enter a traffic type, settings appear for broadcast storm control.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of a partial output from the **show storm-control** command when no keywords are entered. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
Gi0/2        Forwarding     50.00%      40.00%     0.00%
<output truncated>
```

This is an example of output from the **show storm-control** command for a specified interface. Because no traffic-type keyword was entered, the broadcast storm control settings appear.

```
Switch> show storm-control gigabitethernet 0/1
Interface    Filter State   Upper       Lower      Current
---------    -------------  ----------  ---------  ---------
Gi0/1        Forwarding     20 pps      10 pps     5 pps
```

Table 2-16 describes the fields in the **show storm-control** display.

*Table 2-16 show storm-control Field Descriptions*

| Field | Description |
|---|---|
| Interface | Displays the ID of the interface. |
| Filter State | Displays the status of the filter:<br>• Blocking—Storm control is enabled, and a storm has occurred.<br>• Forwarding—Storm control is enabled, and no storms have occurred.<br>• Inactive—Storm control is disabled. |
| Upper | Displays the rising suppression level as a percentage of total available bandwidth in packets per second or in bits per second. |
| Lower | Displays the falling suppression level as a percentage of total available bandwidth in packets per second or in bits per second. |
| Current | Displays the bandwidth usage of broadcast traffic or the specified traffic type (broadcast, multicast, or unicast) as a percentage of total available bandwidth. This field is only valid when storm control is enabled. |

## Related Commands

| Command | Description |
|---|---|
| **storm-control** | Sets the broadcast, multicast, or unicast storm control levels for the switch. |

# show system mtu

Use the **show system mtu** privileged EXEC command to display the global maximum transmission unit (MTU) or maximum packet size set for the switch.

**show system mtu** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you have used the **system mtu** or **system mtu jumbo** global configuration command to change the MTU setting, the new setting does not take effect until you reset the switch.

The system MTU refers to ports operating at 10/100 Mbps; the system jumbo MTU refers to Gigabit ports.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show system mtu** command:

```
Switch# show system mtu
System MTU size is 1500 bytes
System Jumbo MTU size is 1500 bytes
```

## Related Commands

| Command | Description |
|---|---|
| system mtu | Sets the MTU size for the Fast Ethernet or Gigabit Ethernet ports. |

# show table-map

Use the **show table-map** user EXEC command to display quality of service (QoS) table-map information about all configured table maps or the specified table map.

**show table-map** [*table-map-name*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *table-map-name* | (Optional) The name of the table map. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show table-map** command:

```
Switch> show table-map
tandoori_1>show table-map
 Table Map abc
    default copy

 Table Map cos2dscp
    from 2 to 16
    default copy

 Table Map cos2cos
    from 2 to 5
    from 3 to 6
    default 7

 Table Map cos2cos10
    default copy

 Table Map cos=cos
    default copy
```

This is an example of output from the **show table-map** command for a specific table map name:

```
Switch> show table-map tm

Table Map tm
    from 1 to 62
    from 2 to 63
    default ignore
```

## Related Commands

| Command | Description |
|---|---|
| table-map | Creates quality of service (QoS) mapping tables, such as CoS to DSCP, and so on. |

# show udld

Use the **show udld** user EXEC command to display UniDirectional Link Detection (UDLD) administrative and operational status for all ports or the specified port.

**show udld** [*interface-id*] [ **|** {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | (Optional) ID of the interface and port number. Valid interfaces include physical ports and VLANs. The VLAN range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not enter an *interface-id*, administrative and operational UDLD status for all interfaces appear.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show udld** *interface-id* command. For this display, UDLD is enabled on both ends of the link, and UDLD detects that the link is bidirectional. Table 2-17 describes the fields in this display.

```
Switch> show udld gigabitethernet0/1
Interface gi0/1
---
Port enable administrative configuration setting: Follows device default
Port enable operational state: Enabled
Current bidirectional state: Bidirectional
Current operational state: Advertisement - Single Neighbor detected
Message interval: 60
Time out interval: 5
    Entry 1
    Expiration time: 146
    Device ID: 1
    Current neighbor state: Bidirectional
    Device name: Switch-A
    Port ID: Gi0/1
    Neighbor echo 1 device: Switch-B
    Neighbor echo 1 port: Gi0/2
    Message interval: 5
    CDP Device name: Switch-A
```

*Table 2-17 show udld Field Descriptions*

| Field | Description |
|---|---|
| Interface | The interface on the local device configured for UDLD. |
| Port enable administrative configuration setting | How UDLD is configured on the port. If UDLD is enabled or disabled, the port enable configuration setting is the same as the operational enable state. Otherwise, the enable operational setting depends on the global enable setting. |
| Port enable operational state | Operational state that shows whether UDLD is actually running on this port. |
| Current bidirectional state | The bidirectional state of the link. An unknown state appears if the link is down or if it is connected to an UDLD-incapable device. A bidirectional state appears if the link is a normal two-way connection to a UDLD-capable device. All other values mean miswiring. |
| Current operational state | The current phase of the UDLD state machine. For a normal bidirectional link, the state machine is most often in the Advertisement phase. |
| Message interval | How often advertisement messages are sent from the local device. Measured in seconds. |
| Time out interval | The time period, in seconds, that UDLD waits for echoes from a neighbor device during the detection window. |
| Entry 1 | Information from the first cache entry, which contains a copy of echo information received from the neighbor. |
| Expiration time | The amount of time in seconds remaining before this cache entry is aged out. |
| Device ID | The neighbor device identification. |
| Current neighbor state | The neighbor's current state. If both the local and neighbor devices are running UDLD normally, the neighbor state and local state should be bidirectional. If the link is down or the neighbor is not UDLD-capable, no cache entries appear. |
| Device name | The device name or the system serial number of the neighbor. The system serial number appears if the device name is not set or is set to the default (Switch). |
| Port ID | The neighbor port ID enabled for UDLD. |
| Neighbor echo 1 device | The device name of the neighbors' neighbor from which the echo originated. |
| Neighbor echo 1 port | The port number ID of the neighbor from which the echo originated. |
| Message interval | The rate, in seconds, at which the neighbor is sending advertisement messages. |
| CDP device name | The CDP device name or the system serial number. The system serial number appears if the device name is not set or is set to the default (Switch). |

**Related Commands**

| Command | Description |
|---|---|
| **udld** | Enables aggressive or normal mode in UDLD or sets the configurable message timer time. |
| **udld port** | Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command. |
| **udld reset** | Resets all interfaces shutdown by UDLD and permits traffic to begin passing through them again. |

# show version

Use the **show version** user EXEC command to display version information for the hardware and firmware.

**show version** [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show version** command:

**Note** Though visible in the **show version** output, the *configuration register* information is not supported on the switch.

```
Switch> show version
Cisco IOS Software, MEAP Software (MEAP-IPSERVICES-M), Experimental Version 12.2
(20050712:084347) [teresang-meap-bug-fix 109]
Copyright (c) 1986-2005 by Cisco Systems, Inc.
Compiled Sun 17-Jul-05 13:19 by teresang

ROM: Bootstrap program is C3750 boot loader
BOOTLDR: ME3400 Boot Loader (me3400-HBOOT-M), Version 12.2 [mbutts-meap2 103]

 tandoori_1 uptime is 1 day, 2 hours, 49 minutes
System returned to ROM by power-on
System image file is "flash:image"

cisco ME-3440-24T-FA (PowerPC405) processor with 118784K/12280K bytes of memory.

Processor board ID FSJC0407862
Last reset from power-on
Target IOS Version 12.2(25)SE
3 Virtual Ethernet interfaces
24 FastEthernet interfaces
2 Gigabit Ethernet interfaces
```

```
The password-recovery mechanism is enabled.

512K bytes of flash-simulated non-volatile configuration memory.
Base ethernet MAC Address       : 00:0B:FC:FF:32:80
Power supply part number        : 341-0149-01
Motherboard serial number       : FHH0848001R
Power supply serial number      : DTH0450000T
System serial number            : FSJC0407862
Top Assembly Part Number        : 800-26552-01
Top Assembly Revision Number    : 05
Hardware Board Revision Number  : 0x01


Switch   Ports  Model              SW Version              SW Image
------   -----  -----              ----------              ----------
*    1   26     ME-3440-24T-FA     12.2(20050712:084347)   MEAP-IPSERVICES-M


Configuration register is 0xF
```

# show vlan

Use the **show vlan** user EXEC command to display the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified) on the switch.

**show vlan** [**access-map** | **brief** | **filter** | **id** *vlan-id* | **mtu** | **name** *vlan-name* | **private-vlan [type]** | **remote-span** | **summary** | **uni-vlan [type]** ] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **access-map** | See the **show vlan access-map** command. |
| **brief** | (Optional) Display one line for each VLAN with the VLAN name, status, and its ports. |
| **filter** | See the **show vlan filter** command. |
| **id** *vlan-id* | (Optional) Display information about a single VLAN identified by VLAN ID number. For *vlan-id*, the range is 1 to 4094. |
| **mtu** | (Optional) Display a list of VLANs and the minimum and maximum transmission unit (MTU) sizes configured on ports in the VLAN. |
| **name** *vlan-name* | (Optional) Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters. |
| **private-vlan [type]** | (Optional) Display information about configured private VLANs, including primary and secondary VLAN IDs, type (community, isolated, or primary) and ports belonging to the private VLAN. Enter **type** (optional) to see only the VLAN ID and the type of private VLAN. |
| **remote-span** | (Optional) Display information about Remote SPAN (RSPAN) VLANs. |
| **summary** | (Optional) Display VLAN summary information. |
| **uni-vlan [type]** | (Optional) Display user network interface-enhanced network interface (UNI-ENI) VLAN information. Enter **type** (optional) to see only the VLAN ID and type of UNI-ENI VLAN. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help string, the **ifindex** and **internal usage** keywords are not supported.

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

In the **show vlan mtu** command output, the MTU_Mismatch column shows whether all the ports in the VLAN have the same MTU. When *yes* appears in this column, it means that the VLAN has ports with different MTUs. Packets that are switched from a port with a larger MTU to a port with a smaller MTU might be dropped. If the VLAN does not have a switch virtual interface (SVI), the hyphen (-) symbol appears in the SVI_MTU column. If the MTU-Mismatch column displays *yes*, the names of the port with the MinMTU and the port with the MaxMTU appear.

If you try to associate a private VLAN secondary VLAN with a primary VLAN before you define the secondary VLAN, the secondary VLAN is not included in the **show vlan private-vlan** command output.

In the **show vlan private-vlan type** command output, a *normal* type means a VLAN has a private VLAN association but is not part of the private VLAN. For example, if you define and associate two VLANs as primary and secondary VLANs and then delete the secondary VLAN configuration but do not remove the association from the primary VLAN, the VLAN that was the secondary VLAN is shown as *normal* in the display. In the **show vlan private-vlan** output, the primary and secondary VLAN pair is shown as *non-operational*.

In the **show vlan uni-vlan type** command output, type is either *community* or *isolated*. User network interfaces (UNIs) or enhanced network interfaced (ENIs) in a UNI-ENI community VLAN can communicate with each other; UNIs or ENIs in a UNI-ENI isolated VLAN cannot communicate. Network node interfaces (NNIs) can communicate with each other and with UNIs or ENIs in UNI-ENI isolated and community VLANs.

Expressions are case sensitive. For example, if you enter | **exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show vlan** command. Table 2-18 describes the fields in the display.

**Note** The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not supported or used.

```
Switch> show vlan
Switch#show vlan
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                                Fa0/5, Fa0/6, Fa0/7, Fa0/8
                                                Fa0/9, Fa0/10, Fa0/11, Fa0/12
                                                Fa0/13, Fa0/14, Fa0/15, Fa0/16
                                                Fa0/17, Fa0/18, Fa0/19, Fa0/20
                                                Fa0/21, Fa0/22, Fa0/23, Fa0/24
                                                Gi0/1, Gi0/2
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
```

```
VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
1    enet  100001     1500  -      -      -        -    -        0      0
1002 fddi  101002     1500  -      -      -        -    -        0      0
1003 tr    101003     1500  -      -      -        -    -        0      0
1004 fdnet 101004     1500  -      -      -        ieee -        0      0
1005 trnet 101005    1500  -    -     -      ibm  -      0     0VLAN Name

Remote SPAN VLANs
------------------------------------------------------------------------------

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------

VLAN Type              Ports
---------- ----------------- ----------------------------------------
```

***Table 2-18 show vlan Command Output Fields***

| Field | Description |
|---|---|
| VLAN | VLAN number. |
| Name | Name, if configured, of the VLAN. |
| Status | Status of the VLAN (active or suspend). |
| Ports | Ports that belong to the VLAN. |
| Type | Media type of the VLAN. |
| SAID | Security association ID value for the VLAN. |
| MTU | Maximum transmission unit size for the VLAN. |
| Parent | Parent VLAN, if one exists. |
| RingNo | Ring number for the VLAN, if applicable. |
| BrdgNo | Bridge number for the VLAN, if applicable. |
| Stp | Spanning Tree Protocol type used on the VLAN. |
| BrdgMode | Bridging mode for this VLAN—possible values are source-route bridging (SRB) and source-route transparent (SRT); the default is SRB. |
| Trans1 | Translation bridge 1. |
| Trans2 | Translation bridge 2. |
| Remote SPAN VLANs | Identifies any RSPAN VLANs that have been configured. |
| Primary/Secondary/ Type/Ports | Includes any configured private VLANs, including the primary VLAN ID, the secondary VLAN ID, the type of secondary VLAN (community or isolated), and the ports that belong to it. |
| VLAN Type/Ports | Displays any configured UNI-ENI VLANs, the type (community or isolated), and the ports that belong to it. |

This is an example of output from the **show vlan private-vlan** command:

```
Switch> show vlan private-vlan
Primary Secondary Type              Ports
------- --------- ----------------- ------------------------------------------
10      501       isolated          Gi0/3
10      502       community         Fa0/11
10      503       non-operational3      -
20       25       isolated          Fa0/13, Fa0/20, Fa0/22, Gi0/1,
20       30       community         Fa0/13, Fa0/20, Fa0/21, Gi0/1,
20       35       community         Fa0/13, Fa0/20, Fa0/23, Fa0/33. Gi0/1,
20       55       non-operational
2000   2500       isolated          Fa0/5, Fa0/10, Fa0/15
```

This is an example of output from the **show vlan private-vlan type** command:

```
Switch> show vlan private-vlan type
Vlan Type
---- -----------------
10   primary
501  isolated
502  community
503  normal
```

This is an example of output from the **show vlan uni-vlan type** command:

```
Switch> show vlan uni-vlan type
Vlan Type
---- -----------------
1    UNI isolated
20   UNI community
201  UNI isolated
```

This is an example of output from the **show vlan summary** command:

```
Switch> show vlan summary
Number of existing VLANs           : 45
 Number of existing VTP VLANs      : 0
 Number of existing extended VLANs : 0
```

This is an example of output from the **show vlan id** command.

```
Switch# show vlan id 2
VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
2    enet  100002     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled
```

**Related Commands**

| Command | Description |
|---|---|
| **private-vlan** | Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs. |
| **switchport mode** | Configures the VLAN membership mode of a port. |
| **vlan** | Enables VLAN configuration mode where you can configure VLANs 1 to 4094. |

# show vlan access-map

Use the **show vlan access-map** privileged EXEC command to display information about a particular VLAN access map or for all VLAN access maps.

**show vlan access-map** [*mapname*] [ **|** {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *mapname* | (Optional) Name of a specific VLAN access map. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show vlan access-map** command:

```
Switch# show vlan access-map
Vlan access-map "SecWiz"  10
  Match clauses:
    ip  address: SecWiz_Fa1_0_3_in_ip
  Action:
    forward
```

## Related Commands

| Command | Description |
|---|---|
| **show vlan filter** | Displays information about all VLAN filters or about a particular VLAN or VLAN access map. |
| **vlan access-map** | Creates a VLAN map entry for VLAN packet filtering. |
| **vlan filter** | Applies a VLAN map to one or more VLANs. |

# show vlan filter

Use the **show vlan filter** privileged EXEC command to display information about all VLAN filters or about a particular VLAN or VLAN access map.

**show vlan filter** [**access-map** *name* | **vlan** *vlan-id*] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **access-map** *name* | (Optional) Display filtering information for the specified VLAN access map. |
| **vlan** *vlan-id* | (Optional) Display filtering information for the specified VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show vlan filter** command:

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
  20-22
```

**Related Commands**

| Command | Description |
|---|---|
| **show vlan access-map** | Displays information about a particular VLAN access map or for all VLAN access maps. |
| **vlan access-map** | Creates a VLAN map entry for VLAN packet filtering. |
| **vlan filter** | Applies a VLAN map to one or more VLANs. |

# show vmps

Use the **show vmps** user EXEC command without keywords to display the VLAN Query Protocol (VQP) version, reconfirmation interval, retry count, VLAN Membership Policy Server (VMPS) IP addresses, and the current and primary servers, or use the **statistics** keyword to display client-side statistics.

**show vmps** [**statistics**] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **statistics** | (Optional) Display VQP client-side statistics and counters. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

User EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

This is an example of output from the **show vmps statistics** command.

```
Switch> show vmps statistics
VMPS Client Statistics
----------------------
VQP  Queries:               0
VQP  Responses:             0
VMPS Changes:               0
VQP  Shutdowns:             0
VQP  Denied:                0
VQP  Wrong Domain:          0
VQP  Wrong Version:         0
VQP  Insufficient Resource: 0
```

Table 2-19 describes each field in the display.

*Table 2-19 show vmps statistics Field Descriptions*

| Field | Description |
|---|---|
| VQP Queries | Number of queries sent by the client to the VMPS. |
| VQP Responses | Number of responses sent to the client from the VMPS. |
| VMPS Changes | Number of times that the VMPS changed from one server to another. |

*Table 2-19 show vmps statistics Field Descriptions (continued)*

| Field | Description |
|---|---|
| VQP Shutdowns | Number of times the VMPS sent a response to shut down the port. The client disables the port and removes all dynamic addresses on this port from the address table. You must administratively re-enable the port to restore connectivity. |
| VQP Denied | Number of times the VMPS denied the client request for security reasons. When the VMPS response denies an address, no frame is forwarded to or from the workstation with that address (broadcast or multicast frames are delivered to the workstation if the port has been assigned to a VLAN). The client keeps the denied address in the address table as a blocked address to prevent more queries from being sent to the VMPS for each new packet received from this workstation. The client ages the address if no new packets are received from this workstation on this port within the aging time period. |
| VQP Wrong Domain | Number of times the management domain in the request does not match the one for the VMPS. Any previous VLAN assignments of the port are not changed. This response means that the server and the client have not been configured with the same VQP management domain. |
| VQP Wrong Version | Number of times the version field in the query packet contains a value that is higher than the version supported by the VMPS. The VLAN assignment of the port is not changed. The switches send only VMPS Version 1 requests. |
| VQP Insufficient Resource | Number of times the VMPS is unable to answer the request because of a resource availability problem. If the retry limit has not yet been reached, the client repeats the request with the same server or with the next alternate server, depending on whether the per-server retry count has been reached. |

**Related Commands**

| Command | Description |
|---|---|
| **clear vmps statistics** | Clears the statistics maintained by the VQP client. |
| **vmps reconfirm (privileged EXEC)** | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |
| **vmps retry** | Configures the per-server retry count for the VQP client. |
| **vmps server** | Configures the primary VMPS and up to three secondary servers. |

# shutdown

Use the **shutdown** interface configuration command to disable an interface. Use the **no** form of this command to restart a disabled interface.

**shutdown**

**no shutdown**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **shutdown** command causes a port to stop forwarding. The default state for a user network interface (UNI) or enhanced network interface (ENI) is shut down. Before you can configure a UNI or ENI, you must enable it with the **no shutdown** command. Network node interfaces (NNIs) are enabled by default.

The **no shutdown** command has no effect if the port is a static-access port assigned to a VLAN that has been deleted, suspended, or shut down. The port must first be a member of an active VLAN before it can be re-enabled.

The **shutdown** command disables all functions on the specified interface.

This command also marks the interface as unavailable. To see if an interface is disabled, use the **show interfaces** privileged EXEC command. An interface that has been shut down is shown as administratively down in the display.

## Examples

These examples show how to disable and re-enable a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# shutdown

Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no shutdown
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show interfaces | Displays the statistical information specific to all interfaces or to a specific interface. |

# shutdown vlan

Use the **shutdown vlan** global configuration command to shut down (suspend) local traffic on the specified VLAN. Use the **no** form of this command to restart local traffic on the VLAN.

**shutdown vlan** *vlan-id*

**no shutdown vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | ID of the VLAN to be locally shut down. The range is 2 to 1001. VLANs defined as default VLANs (1 and 1002 to 1005), as well as extended-range VLANs (greater than 1005) cannot be shut down. |

## Defaults

No default is defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the shutdown VLAN configuration command to shut down local traffic on any VLAN, including extended-range VLANs (1006-4094).

## Examples

This example shows how to shut down traffic on VLAN 2:

```
Switch(config)# shutdown vlan 2
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **shutdown** (VLAN configuration) | Shuts down local traffic on the VLAN when in VLAN configuration mode (accessed by the **vlan** *vlan-id* global configuration command). |

# small-frame violation rate

Use the **small-frame violation rate** *pps* interface configuration command on the switch stack or on a standalone switch to configure the rate (threshold) for an interface to be error disabled when it receives VLAN-tagged packets that are small frames (67 bytes or less) at the specified rate. Use the **no** form of this command to return to the default setting.

**small-frame violation rate** *pps*

**no small-frame violation rate** *pps*

## Syntax Description

| | |
|---|---|
| *pps* | Specify the threshold at which an interface receiving small frames will be error disabled. The range is 1 to 10,000 packets per second (pps). |

## Defaults

This feature is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command was introduced. |

## Usage Guidelines

This command enables the rate (threshold) for a port to be error disabled when it receives small frames. Small frames are considered packets that are 67 frames or less.

Use the **errdisable detect cause small-frame** global configuration command to globally enable the small-frames threshold for each port.

You can configure the port to be automatically re-enabled by using the **errdisable recovery cause small-frame** global configuration command. You configure the recovery time by using the **errdisable recovery interval** *interval global configuration command.*

## Examples

This example shows how to enable the small-frame arrival rate feature so that the port is error disabled if incoming small frames arrived at 10,000 pps.

```
Switch(config)# interface gigabitethernet2/0/1
Switch(config-if)# small-frame violation rate 10000
```

You can verify your setting by entering the privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **errdisable detect cause small-frame** | Allows any switch port to be put into the error-disabled state if an incoming frame is smaller than the minimum size and arrives at the specified rate (threshold). |
| **errdisable recovery cause small-frame** | **Enables the recovery timer.** |
| **show interfaces** | Displays the interface settings on the switch, including input and output flow control. |

# snmp-server enable traps

Use the **snmp-server enable traps** global configuration command to enable the switch to send Simple Network Management Protocol (SNMP) notifications for various traps or inform requests to the network management system (NMS). Use the **no** form of this command to return to the default setting.

**snmp-server enable traps** [**bridge** [**newroot**] [**topologychange**] | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **ethernet** | **flash** | **mac-notification** | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete**]

**no snmp-server enable traps** [**bridge** [**newroot**] [**topologychange**] | **config** | **copy-config** | **entity** | **envmon** [**fan** | **shutdown** | **status** | **supply** | **temperature**] | **ethernet** | **flash** | **mac-notification** | **port-security** [**trap-rate** *value*] | **rtr** | **snmp** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**] | **storm-control trap-rate** *value* | **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | **syslog** | **tty** | **vlan-membership** | **vlancreate** | **vlandelete**]

## Syntax Description

| | |
|---|---|
| **bridge** [**newroot**] [**topologychange**] | (Optional) Generate Spanning Tree Protocol (STP) bridge MIB traps. The keywords have these meanings:<br>• **newroot**—(Optional) Enable SNMP STP bridge MIB new root traps.<br>• **topologychange**—(Optional) Enable SNMP STP bridge MIB topology change traps. |
| **config** | (Optional) Enable SNMP configuration traps. |
| **copy-config** | (Optional) Enable SNMP copy-configuration traps. |
| **entity** | (Optional) Enable SNMP entity traps. |
| **envmon** [**fan** \| **shutdown** \| **status** \| **supply** \| **temperature**] | Optional) Enable SNMP environmental traps. The keywords have these meanings:<br>• **fan**—(Optional) Enable fan traps.<br>• **shutdown**—(Optional) Enable environmental monitor shutdown traps.<br>• **status**—(Optional) Enable SNMP environmental status-change traps.<br>• **supply**—(Optional) Enable environmental monitor power-supply traps.<br>• **temperature**—(Optional) Enable environmental monitor temperature traps. |
| **ethernet** | (Optional) Enable SNMP Ethernet traps. |
| **flash** | (Optional) Enable SNMP flash notifications. |
| **mac-notification** | (Optional) Enable MAC address notification traps. |
| **port-security** [**trap-rate** *value*] | (Optional) Enable port security traps. Use the **trap-rat**e keyword to set the maximum number of port-security traps sent per second. The range is from 0 to 1000; the default is 0 (no limit imposed; a trap is sent at every port-security occurrence). |
| **rtr** | (Optional) Enable SNMP Response Time Reporter traps. |

| | |
|---|---|
| **snmp** [**authentication** \| **coldstart** \| **linkdown** \| **linkup** \| **warmstart**] | (Optional) Enable SNMP traps. The keywords have these meanings:<br>• **authentication**—(Optional) Enable authentication trap.<br>• **coldstart**—(Optional) Enable cold-start trap.<br>• **linkdown**—(Optional) Enable linkdown trap.<br>• **linkup**—(Optional) Enable linkup trap.<br>• **warmstart**—(Optional) Enable warm-start trap. |
| **storm-control trap-rate** *value* | (Optional) Enable storm-control traps. Use the **trap-rat**e keyword to set the maximum number of storm-control traps sent per second. The range is from 0 to 1000; the default is 0 (no limit is imposed; a trap is sent at every storm-control occurrence). |
| **stpx** [**inconsistency**] [**root-inconsistency**] [**loop-inconsistency**] | (Optional) Enable SNMP STPX MIB traps. The keywords have these meanings:<br>• **inconsistency**—(Optional) Enable SNMP STPX MIB inconsistency update traps.<br>• **root-inconsistency**—(Optional) Enable SNMP STPX MIB root inconsistency update traps.<br>• **loop-inconsistency**—(Optional) Enable SNMP STPX MIB loop inconsistency update traps. |
| **syslog** | (Optional) Enable SNMP syslog traps. |
| **tty** | (Optional) Send TCP connection traps. This is enabled by default. |
| **vlan-membership** | (Optional) Enable SNMP VLAN membership traps. |
| **vlancreate** | (Optional) Enable SNMP VLAN-created traps. |
| **vlandelete** | (Optional) Enable SNMP VLAN-deleted traps. |

**Note** Though visible in the command-line help strings, the **cpu** [**threshold**], **fru-ctrl insertion** and **removal**, and **vtp** keywords are not supported. The **snmp-server enable informs** global configuration command is not supported. To enable the sending of SNMP inform notifications, use the **snmp-server enable traps** global configuration command combined with the **snmp-server host** *host-addr* **informs** global configuration command.

## Defaults

The sending of SNMP traps is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Specify the host (NMS) that receives the traps by using the **snmp-server host** global configuration command. If no trap types are specified, all trap types are sent.

When supported, use the **snmp-server enable traps** command to enable sending of traps or informs.

**Note** Informs are not supported in SNMPv1.

To enable more than one type of trap, you must enter a separate **snmp-server enable traps** command for each trap type.

## Examples

This example shows how to send port security traps to the NMS:

```
Switch(config)# snmp-server enable traps port security
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **snmp-server host** | Specifies the host that receives SNMP traps. |

# snmp-server host

Use the **snmp-server host** global configuration command to specify the recipient (host) of a Simple Network Management Protocol (SNMP) notification operation. Use the **no** form of this command to remove the specified host.

**snmp-server host** *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth| priv**}] [**vrf** *vrf-instance*] {*community-string* [*notification-type*]}

**no snmp-server host** *host-addr* [**informs | traps**] [**version** {**1 | 2c | 3** {**auth | noauth | priv**}] [**vrf** *vrf-instance*] *community-string*

## Syntax Description

| | |
|---|---|
| *host-addr* | Name or Internet address of the host (the targeted recipient). |
| **udp-port** *port* | (Optional) Configure the User Datagram Protocol (UDP) port number of the host to receive the traps. The range is from 0 to 65535. |
| **informs | traps** | (Optional) Send SNMP traps or informs to this host. |
| **version 1 | 2c | 3** | (Optional) Version of the SNMP used to send the traps.<br>These keywords are supported:<br>**1**—SNMPv1. This option is not available with informs.<br>**2c**—SNMPv2C.<br>**3**—SNMPv3. These optional keywords can follow the Version 3 keyword:<br>• **auth** (Optional). Enables Message Digest 5 (MD5) and Secure Hash Algorithm (SHA) packet authentication.<br>• **noauth** (Default). The noAuthNoPriv security level. This is the default if the [**auth | noauth | priv**] keyword choice is not specified.<br>• **priv** (Optional). Enables Data Encryption Standard (DES) packet encryption (also called *privacy*).<br>**Note** The **priv** keyword is available only when the cryptographic (encrypted) software image is installed. |
| **vrf** *vrf-instance* | (Optional) Virtual private network (VPN) routing instance and name for this host. |
| *community-string* | Password-like community string sent with the notification operation. Though you can set this string by using the **snmp-server host** command, we recommend that you define this string by using the **snmp-server community** global configuration command before using the **snmp-server host** command. |

| | |
|---|---|
| *notification-type* | (Optional) Type of notification to be sent to the host. If no type is specified, all notifications are sent. The notification type can be one or more of the these keywords:<br>• **bridge**—Send SNMP Spanning Tree Protocol (STP) bridge MIB traps.<br>• **config**—Send SNMP configuration traps.<br>• **copy-config**—Send SNMP copy configuration traps.<br>• **entity**— Send SNMP entity traps.<br>• **envmon**—Send environmental monitor traps.<br>• **flash**—Send SNMP FLASH notifications.<br>• **mac-notification—**Send SNMP MAC notification traps.<br>• **port-security—**Send SNMP port-security traps.<br>• **rtr—**Send SNMP Response Time Reporter traps.<br>• **snmp—**Send SNMP-type traps.<br>• **storm-control—**Send SNMP storm-control traps.<br>• **stpx—**Send SNMP STP extended MIB traps.<br>• **syslog—**Send SNMP syslog traps.<br>• **tty—**Send TCP connection traps.<br>• **vlan-membership—** Send SNMP VLAN membership traps.<br>• **vlancreate—**Send SNMP VLAN-created traps.<br>• **vlandelete—**Send SNMP VLAN-deleted traps. |

**Note** Though visible in the command-line help strings, the **cpu**, **fru-ctrl**, and **vtp** keywords are not supported.

## Defaults

This command is disabled by default. No notifications are sent.

If you enter this command with no keywords, the default is to send all trap types to the host. No informs are sent to this host.

If no **version** keyword is present, the default is Version 1.

If Version 3 is selected and no authentication keyword is entered, the default is the **noauth** (noAuthNoPriv) security level.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

SNMP notifications can be sent as traps or inform requests. Traps are unreliable because the receiver does not send acknowledgments when it receives traps. The sender cannot determine if the traps were received. However, an SNMP entity that receives an inform request acknowledges the message with an SNMP response PDU. If the sender never receives the response, the inform request can be sent again. Thus, informs are more likely to reach their intended destinations.

However, informs consume more resources in the agent and in the network. Unlike a trap, which is discarded as soon as it is sent, an inform request must be held in memory until a response is received or the request times out. Traps are also sent only once, but an inform might be retried several times. The retries increase traffic and contribute to a higher overhead on the network.

If you do not enter an **snmp-server host** command, no notifications are sent. To configure the switch to send SNMP notifications, you must enter at least one **snmp-server host** command. If you enter the command with no keywords, all trap types are enabled for the host. To enable multiple hosts, you must enter a separate **snmp-server host** command for each host. You can specify multiple notification types in the command for each host.

If a local user is not associated with a remote host, the switch does not send informs for the **auth** (authNoPriv) and the **priv** (authPriv) authentication levels.

When multiple **snmp-server host** commands are given for the same host and kind of notification (trap or inform), each succeeding command overwrites the previous command. Only the last **snmp-server host** command is in effect. For example, if you enter an **snmp-server host inform** command for a host and then enter another **snmp-server host inform** command for the same host, the second command replaces the first.

The **snmp-server host** command is used with the **snmp-server enable traps** global configuration command. Use the **snmp-server enable traps** command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one **snmp-server enable traps** command and the **snmp-server host** command for that host must be enabled. Some notification types cannot be controlled with the **snmp-server enable traps** command. For example, some notification types are always enabled. Other notification types are enabled by a different command.

The **no snmp-server host** command with no keywords disables traps, but not informs, to the host. To disable informs, use the **no snmp-server host informs** command.

## Examples

This example shows how to configure a unique SNMP community string named *comaccess* for traps and prevent SNMP polling access with this string through access-list 10:

```
Switch(config)# snmp-server community comaccess ro 10
Switch(config)# snmp-server host 172.20.2.160 comaccess
Switch(config)# access-list 10 deny any
```

This example shows how to send the SNMP traps to the host specified by the name *myhost.cisco.com*. The community string is defined as *comaccess*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com comaccess snmp
```

This example shows how to enable the switch to send all traps to the host *myhost.cisco.com* by using the community string *public*:

```
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server host myhost.cisco.com public
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **snmp-server enable traps** | Enables SNMP notification for various trap types or inform requests. |

# snmp trap mac-notification

Use the **snmp trap mac-notification** interface configuration command to enable the Simple Network Management Protocol (SNMP) MAC address notification trap on a specific Layer 2 interface. Use the **no** form of this command to return to the default setting.

**snmp trap mac-notification** {**added | removed**}

**no snmp trap mac-notification** {**added | removed**}

## Syntax Description

| | |
|---|---|
| **added** | Enable the MAC notification trap whenever a MAC address is added on this interface. |
| **removed** | Enable the MAC notification trap whenever a MAC address is removed from this interface. |

## Defaults

By default, the traps for both address addition and address removal are disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Even though you enable the notification trap for a specific interface by using the **snmp trap mac-notification** command, the trap is generated only when you enable the **snmp-server enable traps mac-notification** and the **mac address-table notification** global configuration commands.

## Examples

This example shows how to enable the MAC notification trap when a MAC address is added to a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# snmp trap mac-notification added
```

You can verify your settings by entering the **show mac address-table notification interface** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **clear mac address-table notification** | Clears the MAC address notification global counters. |
| **mac address-table notification** | Enables the MAC address notification feature. |
| **show mac address-table notification** | Displays the MAC address notification settings for all interfaces or on the specified interface when the **interface** keyword is appended. |
| **snmp-server enable traps** | Sends the SNMP MAC notification traps when the **mac-notification** keyword is appended. |

# spanning-tree

Use the **spanning-tree** interface configuration command with no keywords on an enhanced network interface (ENI) to enable a spanning-tree instance on the interface. Use the **no** form of this command to return to the default setting of disabled.

**spanning-tree**

**no spanning-tree**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The Spanning-Tree Protocol (STP) is disabled on ENIs.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(44)SE | This command (without keywords) was introduced. |

## Usage Guidelines

This command is supported only on ENIs and on EtherChannel port channels that contain ENIs.

STP is not supported on user network interfaces (UNIs) and it is disabled by default on ENIs. Use this command to enable SPT on an ENI. To set a port as an ENI, enter the **port-type eni** interface configuration command. Once STP is enabled on an ENI, all other STP interface configuration commands are available on the interface.

The switch supports only one spanning-tree instance on a VLAN. When NNIs and ENIs with spanning tree enabled are in the same VLAN, they belong to the same spanning-tree instance.

STP is enabled by default on NNIs. UNIs are typically customer-facing ports and do not participate in the spanning tree of the service provider. However, if you configure a customer-facing port as an ENI and enable spanning tree, the ENI could become the spanning tree root port unless you configure root guard on the port by using the **spanning-tree guard root** interface configuration command. A customer-facing ENI with STP enabled participates in the same spanning tree as the service-provider facing NNI.

**Note** Exercise caution when enabling STP on a customer-facing ENI.

## Examples

This example shows how to enable STP on a port:

```
Switch(config)# interface fastethernet0/1
Switch(config-if)# port-type eni
Switch(config-if)# spanning-tree
```

You can verify your setting by entering the **show spanning-tree interface** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show spanning-tree interface** *interface-id* | Display spanning-tree information for the specified interface. |

# spanning-tree bpdufilter

Use the **spanning-tree bpdufilter** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to prevent the interface from sending or receiving bridge protocol data units (BPDUs). Use the **no** form of this command to return to the default setting.

**spanning-tree bpdufilter** {**disable** | **enable**}

**no spanning-tree bpdufilter**

## Syntax Description

| | |
|---|---|
| **disable** | Disable BPDU filtering on the specified STP port. |
| **enable** | Enable BPDU filtering on the specified STP port. |

## Defaults

BPDU filtering is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU filtering only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can enable the BPDU filtering feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

**Caution** Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

You can globally enable BPDU filtering on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpdufilter default** global configuration command.

You can use the **spanning-tree bpdufilter** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpdufilter default** global configuration command.

## Examples

This example shows how to enable the BPDU filtering feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpdufilter enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an STP port and all its associated VLANs. |

# spanning-tree bpduguard

Use the **spanning-tree bpduguard** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to put the interface in the error-disabled state when it receives a bridge protocol data unit (BPDU). Use the **no** form of this command to return to the default setting.

**spanning-tree bpduguard** {**disable** | **enable**}

**no spanning-tree bpduguard**

## Syntax Description

| | |
|---|---|
| **disable** | Disable BPDU guard on the specified STP port. |
| **enable** | Enable BPDU guard on the specified STP port. |

## Defaults

BPDU guard is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure BPDU guard only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an interface from being included in the spanning-tree topology.

You can enable the BPDU guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

You can globally enable BPDU guard on all Port Fast-enabled STP ports by using the **spanning-tree portfast bpduguard default** global configuration command.

You can use the **spanning-tree bpduguard** interface configuration command on an STP port to override the setting of the **spanning-tree portfast bpduguard default** global configuration command.

## Examples

This example shows how to enable the BPDU guard feature on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree bpduguard enable
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an STP port and all its associated VLANs. |

# spanning-tree cost

Use the **spanning-tree cost** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to set the path cost for spanning-tree calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to place in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree** [**vlan** *vlan-id*] **cost** *cost*

**no spanning-tree** [**vlan** *vlan-id*] **cost**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| *cost* | Path cost. The range is 1 to 200000000, with higher values meaning higher costs. |

## Defaults

The default path cost is computed from the STP port bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—4
- 100 Mbps—19
- 10 Mbps—100

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree cost only on NNIs or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When you configure the cost, higher values represent higher costs.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **cost** *cost* command and the **spanning-tree cost** *cost* command, the **spanning-tree vlan** *vlan-id* **cost** *cost* command takes effect.

## Examples

This example shows how to set the path cost to 250 on a port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# spanning-tree cost 250
```

This example shows how to set a path cost to 300 for VLANs 10, 12 to 15, and 20:

```
Switch(config-if)# spanning-tree vlan 10,12-15,20 cost 300
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree interface** *interface-id* | Displays spanning-tree information for the specified interface. |
| **spanning-tree port-priority** | Configures an STP port priority. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree etherchannel guard misconfig

Use the **spanning-tree etherchannel guard misconfig** global configuration command to display an error message when the switch detects an EtherChannel misconfiguration. Use the **no** form of this command to disable the feature.

**spanning-tree etherchannel guard misconfig**

**no spanning-tree etherchannel guard misconfig**

## Syntax Description

This command has no arguments or keywords.

## Defaults

EtherChannel guard is enabled on the switch.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When the switch detects an EtherChannel misconfiguration, this error message appears:

```
PM-4-ERR_DISABLE: Channel-misconfig error detected on [chars], putting [chars] in
err-disable state.
```

To show switch ports that are in the misconfigured EtherChannel, use the **show interfaces status err-disabled** privileged EXEC command. To verify the EtherChannel configuration on a remote device, use the **show etherchannel summary** privileged EXEC command on the remote device.

When a port is in the error-disabled state because of an EtherChannel misconfiguration, you can bring it out of this state by entering the **errdisable recovery cause channel-misconfig** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

## Examples

This example shows how to enable the EtherChannel guard misconfiguration feature:

```
Switch(config)# spanning-tree etherchannel guard misconfig
```

You can verify your settings by entering the **show spanning-tree summary** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **errdisable recovery cause channel-misconfig** | Enables the timer to recover from the EtherChannel misconfiguration error-disable state. |
| **show etherchannel summary** | Displays EtherChannel information for a channel as a one-line summary per channel-group. |
| **show interfaces status err-disabled** | Displays the interfaces in the error-disabled state. |

# spanning-tree extend system-id

Use the **spanning-tree extend system-id** global configuration command to enable the extended system ID feature.

**spanning-tree extend system-id**

**Note** Though visible in the command-line help strings, the **no** version of this command is not supported. You cannot disable the extended system ID feature.

## Syntax Description

This command has no arguments or keywords.

## Defaults

The extended system ID is enabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). This command affects only network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

The switch supports the IEEE 802.1t spanning-tree extensions. Some of the bits previously used for the switch priority are now used for the extended system ID (VLAN identifier for the per-VLAN spanning-tree plus [PVST+] and rapid PVST+ or as an instance identifier for the multiple spanning tree [MST]).

The spanning tree uses the extended system ID, the switch priority, and the allocated spanning-tree MAC address to make the bridge ID unique for each VLAN or multiple spanning-tree instance.

Support for the extended system ID affects how you manually configure the root switch, the secondary root switch, and the switch priority of a VLAN. For more information, see the "spanning-tree mst root" and the "spanning-tree vlan" sections.

If your network consists of switches that do not support the extended system ID and switches that do support it, it is unlikely that the switch with the extended system ID support will become the root switch. The extended system ID increases the switch priority value every time the VLAN number is greater than the priority of the connected switches.

**Related Commands**

| Command | Description |
|---|---|
| **show spanning-tree summary** | Displays a summary of spanning-tree interface states. |
| **spanning-tree mst root** | Configures the MST root switch priority and timers based on the network diameter. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree guard

Use the **spanning-tree guard** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to enable root guard or loop guard on all the VLANs associated with the selected NNI. Root guard restricts which interface is allowed to be the spanning-tree root port or the path-to-the root for the switch. Loop guard prevents alternate or root ports from becoming designated ports when a failure creates a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree guard** {**loop** | **none** | **root**}

**no spanning-tree guard**

## Syntax Description

| | |
|---|---|
| **loop** | Enable loop guard. |
| **none** | Disable root guard or loop guard. |
| **root** | Enable root guard. |

## Defaults

Root guard is disabled.

Loop guard is configured according to the **spanning-tree loopguard default** global configuration command (globally disabled).

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree guard only on NNIs or on enhanced network interfaces ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can enable root guard or loop guard when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

When root guard is enabled, if spanning-tree calculations cause an interface to be selected as the root port, the interface transitions to the root-inconsistent (blocked) state to prevent the customer's switch from becoming the root switch or being in the path to the root. The root port provides the best path from the switch to the root switch.

When the **no spanning-tree guard** or the **no spanning-tree guard none** command is entered, root guard is disabled for all VLANs on the selected NNI. If this interface is in the root-inconsistent (blocked) state, it automatically transitions to the listening state.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate

ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

To disable root guard or loop guard, use the **spanning-tree guard none** interface configuration command on an STP interface. You cannot enable both root guard and loop guard at the same time.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command on an STP interface.

## Examples

This example shows how to enable root guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard root
```

This example shows how to enable loop guard on all the VLANs associated with the specified port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree guard loop
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree loopguard default** | Prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. |
| **spanning-tree mst cost** | Configures the path cost for MST calculations. |
| **spanning-tree mst port-priority** | Configures an STP MST port priority. |
| **spanning-tree mst root** | Configures the MST root switch priority and timers based on the network diameter. |
| **spanning-tree port-priority** | Configures an STP port priority. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree link-type

Use the **spanning-tree link-type** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to override the default link-type setting, which is determined by the duplex mode of the STP port, and to enable rapid spanning-tree transitions to the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree link-type** {**point-to-point** | **shared**}

**no spanning-tree link-type**

## Syntax Description

| | |
|---|---|
| **point-to-point** | Specify that the link type of an STP port is point-to-point. |
| **shared** | Specify that the link type of an STP port is shared. |

## Defaults

The switch derives the link type of an interface from the duplex mode. A full-duplex interface is considered a point-to-point link, and a half-duplex interface is considered a shared link.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree link type only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can override the default setting of the link type by using the **spanning-tree link-type** command. For example, a half-duplex link can be physically connected point-to-point to a single interface on a remote switch running the Multiple Spanning Tree Protocol (MSTP) or the rapid per-VLAN spanning-tree plus (rapid-PVST+) protocol and be enabled for rapid transitions.

## Examples

This example shows how to specify the link type as shared (regardless of the duplex setting) and to prevent rapid transitions to the forwarding state:

```
Switch(config-if)# spanning-tree link-type shared
```

You can verify your setting by entering the **show spanning-tree mst interface** *interface-id* or the show **spanning-tree interface** *interface-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **clear spanning-tree detected-protocols** | Restarts the protocol migration process (force the renegotiation with neighboring switches) on all interfaces or on the specified interface. |
| **show spanning-tree interface** *interface-id* | Displays spanning-tree state information for the specified interface. |
| **show spanning-tree mst interface** *interface-id* | Displays MST information for the specified interface. |

# spanning-tree loopguard default

Use the **spanning-tree loopguard default** global configuration command to enable loopguard by default on all network node interfaces (NNIs) or enhanced network interface (ENIs) with STP enabled. Enabling loopguard prevents alternate or root ports from becoming designated ports because of a failure that leads to a unidirectional link. Use the **no** form of this command to return to the default setting.

**spanning-tree loopguard default**

**no spanning-tree loopguard default**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Loop guard is disabled.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is supported only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

This command has no effect on user network interfaces (UNIs).

You can enable the loop guard feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), rapid-PVST+, or the multiple spanning-tree (MST) mode.

Loop guard is most effective when it is configured on the entire switched network. When the switch is operating in PVST+ or rapid-PVST+ mode, loop guard prevents alternate and root ports from becoming designated ports, and spanning tree does not send bridge protocol data units (BPDUs) on root or alternate ports. When the switch is operating in MST mode, BPDUs are not sent on nonboundary interfaces if the interface is blocked by loop guard in all MST instances. On a boundary interface, loop guard blocks the interface in all MST instances.

Loop guard operates only on STP ports that the spanning tree identifies as point-to-point.

You can override the setting of the **spanning-tree loopguard default** global configuration command by using the **spanning-tree guard loop** interface configuration command.

## Examples

This example shows how to globally enable loop guard:

```
Switch(config)# spanning-tree loopguard default
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree guard loop** | Enables the loop guard feature on all the VLANs associated with the specified STP port. |

# spanning-tree mode

Use the **spanning-tree mode** global configuration command to enable per-VLAN spanning-tree plus (PVST+), rapid PVST+, or multiple spanning tree (MST) on your switch. Use the **no** form of this command to return to the default setting.

**spanning-tree mode** {**mst** | **pvst** | **rapid-pvst**}

**no spanning-tree mode**

## Syntax Description

| | |
|---|---|
| **mst** | Enable MST and Rapid Spanning Tree Protocol (RSTP) (based on IEEE 802.1s and IEEE 802.1w). |
| **pvst** | Enable PVST+ (based on IEEE 802.1D). |
| **rapid-pvst** | Enable rapid PVST+ (based on IEEE 802.1w). |

## Defaults

The default mode is rapid PVST+.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Spanning Tree Protocol (STP) is supported on the switch only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

STP is not supported on user network interfaces (UNIs).

The switch supports PVST+, rapid PVST+, and MSTP, but only one version can be active at any time: All VLANs run PVST+, all VLANs run rapid PVST+, or all VLANs run MSTP.

When you enable the MST mode, RSTP is automatically enabled.

**Caution** Changing spanning-tree modes can disrupt traffic because all spanning-tree instances are stopped for the previous mode and restarted in the new mode.

## Examples

This example shows to enable MST and RSTP on the switch:

```
Switch(config)# spanning-tree mode mst
```

This example shows to enable PVST+ on the switch:

```
Switch(config)# spanning-tree mode pvst
```

You can verify your setting by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# spanning-tree mst configuration

Use the **spanning-tree mst configuration** global configuration command to enter multiple spanning-tree (MST) configuration mode through which you configure the MST region. Use the **no** form of this command to return to the default settings.

**spanning-tree mst configuration**

**no spanning-tree mst configuration**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default mapping is that all VLANs are mapped to the common and internal spanning-tree (CIST) instance (instance 0).

The default name is an empty string.

The revision number is 0.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *instance-id* range changed to 0 to 4094. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in Spanning Tree Protocol (STP).

The **spanning-tree mst configuration** command enables the MST configuration mode. These configuration commands are available:

- **abort**: exits the MST region configuration mode without applying configuration changes.
- **exit**: exits the MST region configuration mode and applies all configuration changes.
- **instance** *instance-id* **vlan** *vlan-range*: maps VLANs to an MST instance. The range for the *instance-id* is 0 to 4094. The range for *vlan-range* is 1 to 4094. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma.
- **name** *name*: sets the configuration name. The *name* string has a maximum length of 32 characters and is case sensitive.
- **no**: negates the **instance**, **name**, and **revision** commands or sets them to their defaults.
- **private-vlan**: Though visible in the command-line help strings, this command is not supported.

- **revision** *version*: sets the configuration revision number. The range is 0 to 65535.
- **show** [**current** | **pending**]: displays the current or pending MST region configuration.

In MST mode, the switch supports up to 16 MST instances. The number of VLANs that can be mapped to a particular MST instance is unlimited.

When you map VLANs to an MST instance, the mapping is incremental, and VLANs specified in the command are added to or removed from the VLANs that were previously mapped. To specify a range, use a hyphen; for example, **instance 1 vlan 1-63** maps VLANs 1 to 63 to MST instance 1. To specify a series, use a comma; for example, **instance 1 vlan 10, 20, 30** maps VLANs 10, 20, and 30 to MST instance 1.

All VLANs that are not explicitly mapped to an MST instance are mapped to the common and internal spanning tree (CIST) instance (instance 0) and cannot be unmapped from the CIST by using the **no** form of the command.

For two or more switches to be in the same MST region, they must have the same VLAN mapping, the same configuration revision number, and the same name.

## Examples

This example shows how to enter MST configuration mode, map VLANs 10 to 20 to MST instance 1, name the region *region1*, set the configuration revision to 1, display the pending configuration, apply the changes, and return to global configuration mode:

```
Switch# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 10-20
Switch(config-mst)# name region1
Switch(config-mst)# revision 1
Switch(config-mst)# show pending
Pending MST configuration
Name      [region1]
Revision  1
Instance  Vlans Mapped
--------  --------------------
0         1-9,21-4094
1         10-20
-------------------------------

Switch(config-mst)# exit
Switch(config)#
```

This example shows how to add VLANs 1 to 100 to the ones already mapped (if any) to instance 2, to move VLANs 40 to 60 that were previously mapped to instance 2 to the CIST instance, to add VLAN 10 to instance 10, and to remove all the VLANs mapped to instance 2 and map them to the CIST instance:

```
Switch(config-mst)# instance 2 vlan 1-100
Switch(config-mst)# no instance 2 vlan 40-60
Switch(config-mst)# instance 10 vlan 10
Switch(config-mst)# no instance 2
```

You can verify your settings by entering the **show pending** MST configuration command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst configuration** | Displays the MST region configuration. |

# spanning-tree mst cost

Use the **spanning-tree mst cost** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) with STP enabled to set the path cost for multiple spanning-tree (MST) calculations. If a loop occurs, spanning tree considers the path cost when selecting an interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **cost** *cost*

**no spanning-tree mst** *instance-id* **cost**

## Syntax Description

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. |
| *cost* | Path cost is 1 to 200000000, with higher values meaning higher costs. |

## Defaults

The default path cost is computed from the interface bandwidth setting. These are the IEEE default path cost values:

- 1000 Mbps—20000
- 100 Mbps—200000
- 10 Mbps—2000000

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *instance-id* range changed to 0 to 4094. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure path cost only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

When you configure the cost, higher values represent higher costs.

## Examples

This example shows how to set a path cost of 250 on a port associated with instances 2 and 4:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 2,4 cost 250
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show spanning-tree mst interface** *interface-id* | Displays MST information for the specified interface. |
| **spanning-tree mst port-priority** | Configures an interface priority. |
| **spanning-tree mst priority** | Configures the switch priority for the specified spanning-tree instance. |

# spanning-tree mst forward-time

Use the **spanning-tree mst forward-time** global configuration command to set the forward-delay time for all multiple spanning-tree (MST) instances. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. Use the **no** form of this command to return to the default setting.

**spanning-tree mst forward-time** *seconds*

**no spanning-tree mst forward-time**

## Syntax Description

| | |
|---|---|
| *seconds* | Length of the listening and learning states. The range is 4 to 30 seconds. |

## Defaults

The default is 15 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning-Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni** | **eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

Changing the **spanning-tree mst forward-time** command affects all spanning-tree instances.

## Examples

This example shows how to set the spanning-tree forwarding time to 18 seconds for all MST instances:

```
Switch(config)# spanning-tree mst forward-time 18
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** | Displays MST information. |
| **spanning-tree mst hello-time** | Sets the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. |
| **spanning-tree mst max-age** | Sets the interval between messages that the spanning tree receives from the root switch. |
| **spanning-tree mst max-hops** | Sets the number of hops in a region before the BPDU is discarded. |

# spanning-tree mst hello-time

Use the **spanning-tree mst hello-time** global configuration command to set the interval between hello bridge protocol data units (BPDUs) sent by root switch configuration messages. Use the **no** form of this command to return to the default setting.

**spanning-tree mst hello-time** *seconds*

**no spanning-tree mst hello-time**

## Syntax Description

| | |
|---|---|
| *seconds* | Interval between hello BPDUs sent by root switch configuration messages. The range is 1 to 10 seconds. |

## Defaults

The default is 2 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning-Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst hello-time** command affects all spanning-tree instances.

## Examples

This example shows how to set the spanning-tree hello time to 3 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst hello-time 3
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** | Displays MST information. |
| **spanning-tree mst forward-time** | Sets the forward-delay time for all MST instances. |
| **spanning-tree mst max-age** | Sets the interval between messages that the spanning tree receives from the root switch. |
| **spanning-tree mst max-hops** | Sets the number of hops in a region before the BPDU is discarded. |

# spanning-tree mst max-age

Use the **spanning-tree mst max-age** global configuration command to set the interval between messages that the spanning tree receives from the root switch. If a switch does not receive a bridge protocol data unit (BPDU) message from the root switch within this interval, it recomputes the spanning-tree topology. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-age** *seconds*

**no spanning-tree mst max-age**

## Syntax Description

| | |
|---|---|
| *seconds* | Interval between messages the spanning tree receives from the root switch. The range is 6 to 40 seconds. |

## Defaults

The default is 20 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25(EX) | This command was introduced. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

After you set the **spanning-tree mst max-age** *seconds* global configuration command, if a switch does not receive BPDUs from the root switch within the specified interval, the switch recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

Changing the **spanning-tree mst max-age** command affects all spanning-tree instances.

## Examples

This example shows how to set the spanning-tree max-age to 30 seconds for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-age 30
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** | Displays MST information. |
| **spanning-tree mst forward-time** | Sets the forward-delay time for all MST instances. |
| **spanning-tree mst hello-time** | Sets the interval between hello BPDUs sent by root switch configuration messages. |
| **spanning-tree mst max-hops** | Sets the number of hops in a region before the BPDU is discarded. |

# spanning-tree mst max-hops

Use the **spanning-tree mst max-hops** global configuration command to set the number of hops in a region before the bridge protocol data unit (BPDU) is discarded and the information held for an interface is aged. Use the **no** form of this command to return to the default setting.

**spanning-tree mst max-hops** *hop-count*

**no spanning-tree mst max-hops**

## Syntax Description

| | |
|---|---|
| *hop-count* | Number of hops in a region before the BPDU is discarded. The range is 1 to 255 hops. |

## Defaults

The default is 20 hops.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *hop-count* range changed to 1 to 255. |

## Usage Guidelines

On the Cisco ME switch, spanning-tree MST configuration is supported only on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

User network interfaces (UNIs) do not participate in STP.

The root switch of the instance always sends a BPDU (or M-record) with a cost of 0 and the hop count set to the maximum value. When a switch receives this BPDU, it decrements the received remaining hop count by one and propagates the decremented count as the remaining hop count in the generated M-records. A switch discards the BPDU and ages the information held for the interface when the count reaches 0.

Changing the **spanning-tree mst max-hops** command affects all spanning-tree instances.

## Examples

This example shows how to set the spanning-tree max-hops to 10 for all multiple spanning-tree (MST) instances:

```
Switch(config)# spanning-tree mst max-hops 10
```

You can verify your setting by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** | Displays MST information. |
| **spanning-tree mst forward-time** | Sets the forward-delay time for all MST instances. |
| **spanning-tree mst hello-time** | Sets the interval between hello BPDUs sent by root switch configuration messages. |
| **spanning-tree mst max-age** | Sets the interval between messages that the spanning tree receives from the root switch. |

# spanning-tree mst port-priority

Use the **spanning-tree mst port-priority** interface configuration command on a network node interface (NNI) or enhanced network interface (ENI) with STP enabled to configure an interface priority. If a loop occurs, the Multiple Spanning Tree Protocol (MSTP) can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **port-priority** *priority*

**no spanning-tree mst** *instance-id* **port-priority**

## Syntax Description

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. |
| *priority* | The range is 0 to 240 in increments of 16. Valid priority values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority. |

## Defaults

The default is 128.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *instance-id* range changed to 0 to 4094. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs). You can configure spanning-tree MST port priority only on NNIs or on ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

You can assign higher priority values (lower numerical values) to STP port that you want selected first and lower priority values (higher numerical values) that you want selected last. If all STP ports have the same priority value, the multiple spanning tree (MST) puts the interface with the lowest interface number in the forwarding state and blocks other interfaces.

## Examples

This example shows how to increase the likelihood that the interface associated with spanning-tree instances 20 and 22 is placed into the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree mst 20,22 port-priority 0
```

You can verify your settings by entering the **show spanning-tree mst interface** *interface-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst interface** *interface-id* | Displays MST information for the specified interface. |
| **spanning-tree mst cost** | Sets the path cost for MST calculations. |
| **spanning-tree mst priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree mst pre-standard

Use the **spanning-tree mst pre-standard** interface configuration command to configure a port to send only prestandard bridge protocol data units (BPDUs).

**spanning-tree mst pre-standard**

**no spanning-tree mst pre-standard**

## Syntax Description

This command has no arguments or keywords.

## Command Default

The default state is automatic detection of prestandard neighbors.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)SEG | This command was introduced. |

## Usage Guidelines

The port can accept both prestandard and standard BPDUs. If the neighbor types are mismatched, only the common and internal spanning tree (CIST) runs on this interface.

**Note** If a switch port is connected to a switch running prestandard Cisco IOS software, you *must* use the **spanning-tree mst pre-standard** interface configuration command on the port. If you do not configure the port to send only prestandard BPDUs, the Multiple STP (MSTP) performance might diminish.

When the port is configured to automatically detect prestandard neighbors, the *prestandard* flag always appears in the **show spanning-tree mst** commands.

## Examples

This example shows how to configure a port to send only prestandard BPDUs:

```
Switch(config-if)# spanning-tree mst pre-standard
```

You can verify your settings by entering the **show spanning-tree mst** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** *instance-id* | Displays multiple spanning-tree (MST) information, including the *prestandard* flag, for the specified interface. |

# spanning-tree mst priority

Use the **spanning-tree mst priority** global configuration command to set the switch priority for the specified spanning-tree instance. Use the **no** form of this command to return to the default setting.

**spanning-tree mst** *instance-id* **priority** *priority*

**no spanning-tree mst** *instance-id* **priority**

## Syntax Description

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. |
| **priority** | Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that the switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.<br>The range is 0 to 61440 in increments of 4096. Valid priority values are 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. |

## Defaults

The default is 32768.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *instance-id* range changed to 0 to 4094. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

## Examples

This example shows how to set the spanning-tree priority to 8192 for multiple spanning-tree instances (MST) 20 to 21:

```
Switch(config)# spanning-tree mst 20-21 priority 8192
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show spanning-tree mst** *instance-id* | Displays MST information for the specified interface. |
| **spanning-tree mst cost** | Sets the path cost for MST calculations. |
| **spanning-tree mst port-priority** | Configures an interface priority. |

# spanning-tree mst root

Use the **spanning-tree mst root** global configuration command to configure the multiple spanning-tree (MST) root switch priority and timers based on the network diameter. Use the **no** form of this command to return to the default settings.

**spanning-tree mst** *instance-id* **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]

**no spanning-tree mst** *instance-id* **root**

## Syntax Description

| | |
|---|---|
| *instance-id* | Range of spanning-tree instances. You can specify a single instance, a range of instances separated by a hyphen, or a series of instances separated by a comma. The range is 0 to 4094. |
| **root primary** | Force this switch to be the root switch. |
| **root secondary** | Set this switch to be the root switch should the primary root switch fail. |
| **diameter** *net-diameter* | (Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. This keyword is available only for MST instance 0. |
| **hello-time** *seconds* | (Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. This keyword is available only for MST instance 0. |

## Defaults

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

The hello time is 2 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The *instance-id* range changed to 0 to 4094. |

## Usage Guidelines

Spanning Tree Protocol (STP) is not supported on user network interfaces (UNIs); it is only supported on network node interfaces (NNIs) or on enhanced network interfaces (ENIs) on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

Use the **spanning-tree mst** *instance-id* **root** command only on backbone switches.

When you enter the **spanning-tree mst** *instance-id* **root** command, the software tries to set a high enough priority to make this switch the root of the spanning-tree instance. Because of the extended system ID support, the switch sets the switch priority for the instance to 24576 if this value will cause

this switch to become the root for the specified instance. If any root switch for the specified instance has a switch priority lower than 24576, the switch sets its own priority to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree mst** *instance-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch fails, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768 and are therefore unlikely to become the root switch).

## Examples

This example shows how to configure the switch as the root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for instance 10 with a network diameter of 4:

```
Switch(config)# spanning-tree mst 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree mst** *instance-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree mst** *instance-id* | Displays MST information for the specified instance. |
| **spanning-tree mst forward-time** | Sets the forward-delay time for all MST instances. |
| **spanning-tree mst hello-time** | Sets the interval between hello BPDUs sent by root switch configuration messages. |
| **spanning-tree mst max-age** | Sets the interval between messages that the spanning tree receives from the root switch. |
| **spanning-tree mst max-hops** | Sets the number of hops in a region before the BPDU is discarded. |

# spanning-tree port-priority

Use the **spanning-tree port-priority** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) on which Spanning Tree Protocol (STP) has been enabled to configure an interface priority. If a loop occurs, spanning tree can find the interface to put in the forwarding state. Use the **no** form of this command to return to the default setting.

**spanning-tree** [**vlan** *vlan-id*] **port-priority** *priority*

**no spanning-tree** [**vlan** *vlan-id*] **port-priority**

## Syntax Description

| | |
|---|---|
| **vlan** *vlan-id* | (Optional) VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| *priority* | Number from 0 to 240, in increments of 16. Valid values are 0, 16, 32, 48, 64, 80, 96, 112, 128, 144, 160, 176, 192, 208, 224, and 240. All other values are rejected. The lower the number, the higher the priority. |

## Defaults

The default is 128.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

STP is not supported on user network interfaces (UNIs). You can configure spanning-tree port priority only on NNIs or on ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

If the variable *vlan-id* is omitted, the command applies to the spanning-tree instance associated with VLAN 1.

You can set the priority on a VLAN that has no interfaces assigned to it. The setting takes effect when you assign the STP port to the VLAN.

If you configure an STP port with both the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command and the **spanning-tree port-priority** *priority* command, the **spanning-tree vlan** *vlan-id* **port-priority** *priority* command takes effect.

## Examples

This example shows how to increase the likelihood that a port will be put in the forwarding state if a loop occurs:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree vlan 20 port-priority 0
```

This example shows how to set the port-priority value on VLANs 20 to 25:

```
Switch(config-if)# spanning-tree vlan 20-25 port-priority 0
```

You can verify your settings by entering the **show spanning-tree interface** *interface-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree interface** *interface-id* | Displays spanning-tree information for the specified interface. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree vlan priority** | Sets the switch priority for the specified spanning-tree instance. |

# spanning-tree portfast (global configuration)

Use the **spanning-tree portfast** global configuration command to globally enable bridge protocol data unit (BPDU) filtering on Port Fast-enabled network node interfaces (NNIs) or enhanced network interfaces (ENIs) on which Spanning Tree Protocol (STP) has been enabled, to enable the BPDU guard feature on Port Fast-enabled STP ports, or the Port Fast feature on all nontrunking STP ports. The BPDU filtering feature prevents the switch STP port from sending or receiving BPDUs. The BPDU guard feature puts Port Fast-enabled STP ports that receive BPDUs in an error-disabled state. Use the **no** form of this command to return to the default settings.

**spanning-tree portfast** {**bpdufilter default** | **bpduguard default** | **default**}

**no spanning-tree portfast** {**bpdufilter default** | **bpduguard default** | **default**}

## Syntax Description

| | |
|---|---|
| **bpdufilter default** | Globally enable BPDU filtering on Port Fast-enabled STP ports, and prevent the switch STP port connected to end stations from sending or receiving BPDUs. |
| **bpduguard default** | Globally enable the BPDU guard feature on Port Fast-enabled STP ports, and place the STP ports that receive BPDUs in an error-disabled state. |
| **default** | Globally enable the Port Fast feature on all nontrunking STP ports. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. |

## Defaults

The BPDU filtering, the BPDU guard, and the Port Fast features are disabled on all NNIs or ENIs unless they are individually configured.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

STP is not supported on user network interfaces (UNIs) on the switch. Spanning-tree configuration affects only NNIs or ENIs on which STP has been enabled. To set a port as an ENI or NNI, enter the **port-type** {**eni** | **nni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

UNIs are typically customer-facing ports and do not participate in the spanning tree of the service provider. However, if you configure a customer-facing port as an ENI and enable spanning tree, the ENI could become the spanning tree root port unless you configure root guard on the port by using the **spanning-tree guard root** interface configuration command. A customer-facing ENI with STP enabled participates in the same spanning tree as the service-provider facing NNI.

**Note** Exercise caution when enabling STP on a customer-facing ENI.

You can enable these features when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

Use the **spanning-tree portfast bpdufilter default** global configuration command to globally enable BPDU filtering on STP ports that are Port Fast-enabled. The STP ports still send a few BPDUs at link-up before the switch begins to filter outbound BPDUs. You should globally enable BPDU filtering on a switch so that hosts connected to switch STP ports do not receive BPDUs. If a BPDU is received on a Port Fast-enabled STP port, the interface loses its Port Fast-operational status and BPDU filtering is disabled.

You can override the **spanning-tree portfast bpdufilter default** global configuration command on an STP port by using the **spanning-tree bdpufilter** interface configuration command.

**Caution** Enabling BPDU filtering on an STP port is the same as disabling spanning tree on it and can result in spanning-tree loops.

Use the **spanning-tree portfast bpduguard default** global configuration command to globally enable BPDU guard on STP ports that are in a Port Fast-operational state. In a valid configuration, Port Fast-enabled STP ports do not receive BPDUs. Receiving a BPDU on a Port Fast-enabled STP port signals an invalid configuration, such as the connection of an unauthorized device, and the BPDU guard feature puts the STP port in the error-disabled state. The BPDU guard feature provides a secure response to invalid configurations because you must manually put the STP port back in service. Use the BPDU guard feature in a service-provider network to prevent an access port from participating in the spanning tree.

You can override the **spanning-tree portfast bpduguard default** global configuration command by using the **spanning-tree bdpuguard** interface configuration command on an STP port.

Use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking STP ports. Configure Port Fast only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation. A Port Fast-enabled STP port moves directly to the spanning-tree forwarding state when linkup occurs without waiting for the standard forward-delay time.

You can override the **spanning-tree portfast default** global configuration command by using the **spanning-tree portfast** interface configuration command on an STP port. You can use the **no spanning-tree portfast default** global configuration command to disable Port Fast on all STP ports unless they are individually configured with the **spanning-tree portfast** interface configuration command.

## Examples

This example shows how to globally enable the BPDU filtering feature:

```
Switch(config)# spanning-tree portfast bpdufilter default
```

This example shows how to globally enable the BPDU guard feature:

```
Switch(config)# spanning-tree portfast bpduguard default
```

This example shows how to globally enable the Port Fast feature on all nontrunking interfaces:

```
Switch(config)# spanning-tree portfast default
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree bpdufilter** | Prevents an interface from sending or receiving BPDUs. |
| **spanning-tree bpduguard** | Puts an STP port in the error-disabled state when it receives a BPDU. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an STP port in all its associated VLANs. |

# spanning-tree portfast (interface configuration)

Use the **spanning-tree portfast** interface configuration command on a network node interface (NNI) or an enhanced network interface (ENI) on which Spanning Tree Protocol (STP) has been enabled to enable the Port Fast feature on an STP port in all its associated VLANs. When the Port Fast feature is enabled, the STP port changes directly from a blocking state to a forwarding state without making the intermediate spanning-tree state changes. Use the **no** form of this command to return to the default setting.

**spanning-tree portfast** [**disable | trunk**]

**no spanning-tree portfast**

## Syntax Description

| | |
|---|---|
| **disable** | (Optional) Disable the Port Fast feature on the specified interface. |
| **trunk** | (Optional) Enable the Port Fast feature on a trunking interface. |

## Defaults

The Port Fast feature is disabled on all ports.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

STP is not supported on user network interfaces (UNIs). You can enable the spanning-tree Port Fast feature only on NNIs or on ENIs on which STP has been enabled. To set a port as an NNI or ENI, enter the **port-type** {**nni | eni**} interface configuration command. To enable STP on an ENI, enter the **spanning-tree** interface configuration command.

Use this feature only on STP ports that connect to end stations; otherwise, an accidental topology loop could cause a data packet loop and disrupt switch and network operation.

To enable Port Fast on trunk ports, you must use the **spanning-tree portfast trunk** interface configuration command. The **spanning-tree portfast** command is not supported on trunk ports.

You can enable this feature when the switch is operating in the per-VLAN spanning-tree plus (PVST+), the rapid-PVST+, or the multiple spanning-tree (MST) mode.

This feature affects all VLANs on the STP port.

An NNI with the Port Fast feature enabled is moved directly to the spanning-tree forwarding state without the standard forward-time delay.

You can use the **spanning-tree portfast default** global configuration command to globally enable the Port Fast feature on all nontrunking interfaces. However, the **spanning-tree portfast** interface configuration command can override the global setting.

If you configure the **spanning-tree portfast default** global configuration command, you can disable Port Fast on an STP port that is not a trunk interface by using the **spanning-tree portfast disable** interface configuration command.

## Examples

This example shows how to enable the Port Fast feature on a port:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# spanning-tree portfast
```

You can verify your settings by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **spanning-tree bpdufilter** | Prevents an interface from sending or receiving bridge protocol data units (BPDUs). |
| **spanning-tree bpduguard** | Puts an interface in the error-disabled state when it receives a BPDU. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports. |

# spanning-tree vlan

Use the **spanning-tree vlan** global configuration command to configure spanning tree on a per-VLAN basis. Use the **no** form of this command to return to the default setting.

**spanning-tree vlan** *vlan-id* [**forward-time** *seconds* | **hello-time** *seconds* | **max-age** *seconds* | **priority** *priority* | **root** {**primary** | **secondary**} [**diameter** *net-diameter* [**hello-time** *seconds*]]]

**no spanning-tree vlan** *vlan-id* [**forward-time** | **hello-time** | **max-age** | **priority** | **root**]

## Syntax Description

| | |
|---|---|
| *vlan-id* | VLAN range associated with a spanning-tree instance. You can specify a single VLAN identified by VLAN ID number, a range of VLANs separated by a hyphen, or a series of VLANs separated by a comma. The range is 1 to 4094. |
| **forward-time** *seconds* | (Optional) Set the forward-delay time for the specified spanning-tree instance. The forwarding time specifies how long each of the listening and learning states last before the interface begins forwarding. The range is 4 to 30 seconds. |
| **hello-time** *seconds* | (Optional) Set the interval between hello bridge protocol data units (BPDUs) sent by the root switch configuration messages. The range is 1 to 10 seconds. |
| **max-age** *seconds* | (Optional) Set the interval between messages the spanning tree receives from the root switch. If a switch does not receive a BPDU message from the root switch within this interval, it recomputes the spanning-tree topology. The range is 6 to 40 seconds. |
| **priority** *priority* | (Optional) Set the switch priority for the specified spanning-tree instance. This setting affects the likelihood that this switch is selected as the root switch. A lower value increases the probability that the switch is selected as the root switch.<br>The range is 0 to 61440 in increments of 4096. Valid priority values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected. |
| **root primary** | (Optional) Force this switch to be the root switch. |
| **root secondary** | (Optional) Set this switch to be the root switch should the primary root switch fail. |
| **diameter** *net-diameter* | (Optional) Set the maximum number of switches between any two end stations. The range is 2 to 7. |

## Defaults

Spanning tree is enabled on all VLANs.

The forward-delay time is 15 seconds.

The hello time is 2 seconds.

The max-age is 20 seconds.

The primary root switch priority is 24576.

The secondary root switch priority is 28672.

**Command Modes** Global configuration

**Command History**

| Release | Modification |
|---|---|
| 12.25(EX) | This command was introduced. |

**Usage Guidelines** The switch does not support Spanning Tree Protocol (STP) on user network interfaces (UNIs). Only the switch network node interfaces (NNIs) or STP-enabled enhanced network interfaces (ENIs) in a VLAN participate in STP.

Disabling the STP causes the VLAN to stop participating in the spanning-tree topology. STP ports that are administratively down remain down. Received BPDUs are forwarded like other multicast frames. The VLAN does not detect and prevent loops when STP is disabled.

You can disable the STP on a VLAN that is not currently active and verify the change by using the **show running-config** or the **show spanning-tree vlan** *vlan-id* privileged EXEC command. The setting takes effect when the VLAN is activated.

When disabling or re-enabling the STP, you can specify a range of VLANs that you want to disable or enable.

When a VLAN is disabled and then enabled, all assigned VLANs continue to be its members. However, all spanning-tree bridge parameters are returned to their previous settings (the last setting before the VLAN was disabled).

You can enable spanning-tree options on a VLAN that has no STP ports assigned to it. The setting takes effect when you assign interfaces to it.

When setting the **max-age** *seconds,* if a switch does not receive BPDUs from the root switch within the specified interval, it recomputes the spanning-tree topology. The **max-age** setting must be greater than the **hello-time** setting.

The **spanning-tree vlan** *vlan-id* **root** command should be used only on backbone switches.

When you enter the **spanning-tree vlan** *vlan-id* **root** command, the software checks the switch priority of the current root switch for each VLAN. Because of the extended system ID support, the switch sets the switch priority for the specified VLAN to 24576 if this value will cause this switch to become the root for the specified VLAN. If any root switch for the specified VLAN has a switch priority lower than 24576, the switch sets its own priority for the specified VLAN to 4096 less than the lowest switch priority. (4096 is the value of the least-significant bit of a 4-bit switch priority value.)

When you enter the **spanning-tree vlan** *vlan-id* **root secondary** command, because of support for the extended system ID, the software changes the switch priority from the default value (32768) to 28672. If the root switch should fail, this switch becomes the next root switch (if the other switches in the network use the default switch priority of 32768, and therefore, are unlikely to become the root switch).

**Examples** This example shows how to disable the STP on VLAN 5:

```
Switch(config)# no spanning-tree vlan 5
```

You can verify your setting by entering the **show spanning-tree** privileged EXEC command. In this instance, VLAN 5 does not appear in the list.

This example shows how to set the spanning-tree forwarding time to 18 seconds for VLANs 20 and 25:

```
Switch(config)# spanning-tree vlan 20,25 forward-time 18
```

This example shows how to set the spanning-tree hello-delay time to 3 seconds for VLANs 20 to 24:

```
Switch(config)# spanning-tree vlan 20-24 hello-time 3
```

This example shows how to set spanning-tree max-age to 30 seconds for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 max-age 30
```

This example shows how to reset the **max-age** parameter to the default value for spanning-tree instance 100 and 105 to 108:

```
Switch(config)# no spanning-tree vlan 100, 105-108 max-age
```

This example shows how to set the spanning-tree priority to 8192 for VLAN 20:

```
Switch(config)# spanning-tree vlan 20 priority 8192
```

This example shows how to configure the switch as the root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root primary diameter 4
```

This example shows how to configure the switch as the secondary root switch for VLAN 10 with a network diameter of 4:

```
Switch(config)# spanning-tree vlan 10 root secondary diameter 4
```

You can verify your settings by entering the **show spanning-tree vlan** *vlan-id* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show spanning-tree vlan** | Displays spanning-tree information. |
| **spanning-tree cost** | Sets the path cost for spanning-tree calculations. |
| **spanning-tree guard** | Enables the root guard or the loop guard feature for all the VLANs associated with the selected interface. |
| **spanning-tree port-priority** | Sets an interface priority. |
| **spanning-tree portfast (global configuration)** | Globally enables the BPDU filtering or the BPDU guard feature on Port Fast-enabled STP ports or enables the Port Fast feature on all nontrunking STP ports. |
| **spanning-tree portfast (interface configuration)** | Enables the Port Fast feature on an STP port in all its associated VLANs. |

# speed

Use the **speed** interface configuration command to specify the speed of a 10/100 Mbps or 10/100/1000 Mbps port. Use the **no** or **default** form of this command to return the port to its default value.

**speed** {**10** | **100** | **1000** | **auto** [**10** | **100** | **1000**] | **nonegotiate**}

**no speed**

**Note** For speed configurations restrictions on small form-factor pluggable (SFP) module ports, see the "Usage Guidelines" section.

**Note** You cannot configure the speed on small form-factor pluggable (SFP) module ports, but you can configure the speed to not negotiate (**nonegotiate**) if they are connected to a device that does not support autonegotiation. See "Usage Guidelines" for exceptions when a 1000BASE-T SFP module is in the SFP module slot.

## Syntax Description

| | |
|---|---|
| **10** | Port runs at 10 Mbps. |
| **100** | Port runs at 100 Mbps. |
| **1000** | Port runs at 1000 Mbps. This option is valid and visible only on 10/100/1000 Mbps-ports. |
| **auto** | Port automatically detects the speed it should run at based on the port at the other end of the link. If you use the **10**, **100**, or **1000** keywords with the **auto** keyword, the port only autonegotiates at the specified speeds. |
| **nonegotiate** | Autonegotiation is disabled, and the port runs at 1000 Mbps. (The 1000BASE-T SFP does not support the **nonegotiate** keyword.) |

## Defaults

The default is **auto**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can configure the Fast Ethernet port speed as either 10 or 100 Mbps.

You can configure the Gigabit Ethernet port speed as 10, 100, or 1000 Mbps.

When a 1000BASE-T SFP module is in the SFP module slot, you can configure the speed as **10**, **100**, **1000**, or auto but not to **nonegotiate**.

Except for the 1000BASE-T SFP modules, if an SFP module port is connected to a device that does not support autonegotiation, you can configure the speed to not negotiate (**nonegotiate**).

If the speed is set to **auto**, the switch negotiates with the device at the other end of the link for the speed setting and then forces the speed setting to the negotiated value. The duplex setting remains as configured on each end of the link, which could result in a duplex setting mismatch.

If both ends of the line support autonegotiation, we highly recommend the default autonegotiation settings. If one interface supports autonegotiation and the other end does not, do use the **auto** setting on the supported side, but set the duplex and speed on the other side.

**Caution** Changing the interface speed and duplex mode configuration might shut down and re-enable the interface during the reconfiguration.

**Note** For guidelines on setting the switch speed and duplex parameters, see the software configuration guide for this release.

## Examples

This example shows how to set speed on a port to 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed 100
```

This example shows how to set a port to autonegotiate at only 10 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10
```

This example shows how to set a port to autonegotiate at only 10 or 100 Mbps:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# speed auto 10 100
```

You can verify your settings by entering the **show interfaces** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **duplex** | Specifies the duplex mode of operation. |
| **show interfaces** | Displays the statistical information specific to all interfaces or to a specific interface. |

# storm-control

Use the **storm-control** interface configuration command to enable broadcast, multicast, or unicast storm control and to set threshold levels on an interface. Use the **no** form of this command to return to the default setting.

**storm-control** {{**broadcast** | **multicast** | **unicast**} **level** {*level* [*level-low*] | **bps** *bps* [*bps-low*] | **pps** *pps* [*pps-low*]}} | {**action** {**shutdown** | **trap**}}

**no storm-control** {{**broadcast** | **multicast** | **unicast**} **level**} | {**action** {**shutdown** | **trap**}}

## Syntax Description

| | |
|---|---|
| **broadcast** | Enable broadcast storm control on the interface. |
| **multicast** | Enable multicast storm control on the interface. |
| **unicast** | Enable unicast storm control on the interface. |
| **level** *level* [*level-low*] | Specify the rising and falling suppression levels as a percentage of total bandwidth of the port.<br>• *level*—Rising suppression level, up to two decimal places. The range is 0.00 to 100.00. Block the flooding of storm packets when the value specified for *level* is reached.<br>• *level-low*—(Optional) Falling suppression level, up to two decimal places. The range is 0.00 to 100.00. This value must be less than or equal to the rising suppression value. If you do not configure a falling suppression level, it is set to the rising suppression level. |
| **level bps** *bps* [*bps-low*] | Specify the rising and falling suppression levels as a rate in bits per second at which traffic is received on the port.<br>• *bps*—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for *bps* is reached.<br>• *bps-low*—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.<br>You can use metric suffixes such as k, m, and g for large number thresholds. |

| | |
|---|---|
| **level pps** *pps* [*pps-low*] | Specify the rising and falling suppression levels as a rate in packets per second at which traffic is received on the port.<br>• *pps*—Rising suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. Block the flooding of storm packets when the value specified for *pps* is reached.<br>• *pps-low*—(Optional) Falling suppression level, up to 1 decimal place. The range is 0.0 to 10000000000.0. This value must be equal to or less than the rising suppression value.<br>You can use metric suffixes such as k, m, and g for large number thresholds. |
| **action** {**shutdown** \| **trap**} | Action taken when a storm occurs on a port. The default action is to filter traffic and to not send an Simple Network Management Protocol (SNMP) trap.<br>The keywords have these meanings:<br>• **shutdown**—Disables the port during a storm.<br>• **trap**—Sends an SNMP trap when a storm occurs. |

## Defaults

Broadcast, multicast, and unicast storm control are disabled.

The default action is to filter traffic and to not send an SNMP trap.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Storm control is supported only on physical interfaces. You can also configure storm control on an EtherChannel. When storm control is configured on an EtherChannel, the storm control settings propagate to the EtherChannel physical interfaces. If the port is a user network interface (UNI) or enhanced network interfaces (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **storm-control** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

The storm-control suppression level can be entered as a percentage of total bandwidth of the port, as a rate in packets per second at which traffic is received, or as a rate in bits per second at which traffic is received.

When specified as a percentage of total bandwidth, a suppression value of 100 percent means that no limit is placed on the specified traffic type. A value of **level 0 0** means that all broadcast, multicast, or unicast traffic on that port is blocked. Storm control is enabled only when the rising suppression level is less than 100 percent. If no other storm-control configuration is specified, the default action is to filter the traffic causing the storm and to send no SNMP traps.

**Note** When the storm control threshold for multicast traffic is reached, all multicast traffic except control traffic, such as bridge protocol data unit (BDPU) and Cisco Discovery Protocol (CDP) frames, are blocked.

The **trap** and **shutdown** options are independent of each other.

If you configure the action to be taken as shutdown (the port is error-disabled during a storm) when a packet storm is detected, you must use the **no shutdown** interface configuration command to bring the interface out of this state. If you do not specify the **shutdown** action, specify the action as **trap** (the switch generates a trap when a storm is detected).

When a storm occurs and the action is to filter traffic, if the falling suppression level is not specified, the switch blocks all traffic until the traffic rate drops below the rising suppression level. If the falling suppression level is specified, the switch blocks traffic until the traffic rate drops below this level.

When a broadcast storm occurs and the action is to filter traffic, the switch blocks only broadcast traffic.

For more information, see the software configuration guide for this release.

## Examples

This example shows how to enable broadcast storm control with a 75.5-percent rising suppression level:

```
Switch(config-if)# storm-control broadcast level 75.5
```

This example shows how to enable unicast storm control on a port with a 87-percent rising suppression level and a 65-percent falling suppression level:

```
Switch(config-if)# storm-control unicast level 87 65
```

This example shows how to enable multicast storm control on a port with a 2000-packets-per-second rising suppression level and a 1000-packets-per-second falling suppression level:

```
Switch(config-if)# storm-control multicast level pps 2k 1k
```

This example shows how to enable the **shutdown** action on a port:

```
Switch(config-if)# storm-control action shutdown
```

You can verify your settings by entering the **show storm-control** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show storm-control | Displays broadcast, multicast, or unicast storm control settings on all interfaces or on a specified interface. |

# switchport

Use the **switchport** interface configuration command with no keywords to put an interface that was processing traffic through the CPU into normal switching mode. Use the **no** form of this command to put an interface in Layer 3 mode.

**switchport**

**no switchport**

## Syntax Description

This command has no arguments or keywords.

## Defaults

By default, all interfaces are in Layer 2 (switching) mode.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use the **no switchport** command (without parameters) to set the interface so that traffic on the interface is processed by the CPU. You must enter the **no switchport** command and then assign an IP address to the port.

If an interface is configured to process traffic through the CPU, you must first enter the **switchport** command with no keywords before configuring switching characteristics on the port. Then you can enter additional **switchport** commands with keywords, as shown on the pages that follow.

Entering the **no switchport** command shuts the port down and then re-enables it, which might generate messages on the device to which the port is connected.

When you enter the **switchport** (or **no switchport**) command without keywords on an interface, the configuration information for the affected interface might be lost, and the interface returned to its default configuration.

## Examples

This example shows how to cause an interface to stop operating as a switching port and process traffic on the port through the CPU.

```
Switch(config-if)# no switchport
```

This example shows how to return the port to switching mode:

```
Switch(config-if)# switchport
```

You can verify the switchport status of an interface by entering the **show running-config** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching (nonrouting) port, including port blocking and port protection settings. |
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |

# switchport access vlan

Use the **switchport access vlan** interface configuration command to configure a port as a static-access or dynamic-access port. If the switchport mode is set to **access** (by using the **switchport mode** interface configuration command), use this command to set the port to operate as a member of the specified VLAN or to specify that the port uses VLAN Membership Policy Server (VMPS) protocol where VLAN assignment based on the incoming packets it receives. Use the **no** form of this command to reset the access VLAN mode to the default VLAN for the switch.

**switchport access vlan** {*vlan-id* | **dynamic**}

**no switchport access vlan**

## Syntax Description

| | |
|---|---|
| *vlan-id* | Configure the interface as a static access port with the VLAN ID of the access mode VLAN; the range is 1 to 4094. |
| **dynamic** | Specify that the access mode VLAN is dependent on the VMPS protocol. The port is assigned to a VLAN based on the source MAC address of a host (or hosts) connected to the port. The switch sends every new MAC address received to the VMPS server to obtain the VLAN name to which the dynamic-access port should be assigned. If the port already has a VLAN assigned and the source has already been approved by the VMPS, the switch forwards the packet to the VLAN.<br>**Note** This keyword is visible only on user network interfaces (UNIs) or enhanced network interfaces (ENIs). |

## Defaults

The default access VLAN and trunk interface native VLAN is a VLAN corresponding to the platform or interface hardware.

A dynamic-access port is initially a member of no VLAN and receives its assignment based on the packet it receives.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **no switchport access vlan** command resets the access mode VLAN to the appropriate default VLAN for the device.

The port must be in access mode before the **switchport access vlan** command can take effect.

An access port can be assigned to only one VLAN.

The VMPS server (such as a Catalyst 6500 series switch) must be configured before a port is configured as dynamic.

If the specified VLAN is configured as a UNI-ENI community VLAN, the interface is configured as UNI-ENI community port. Otherwise the port is configured as a UNI-ENI isolated port.

This command is supported on IEEE802.1Q tunnel ports.

These restrictions apply to dynamic-access ports:

- The **dynamic** keyword is not visible on network node interfaces (NNIs).
- The software implements the VLAN Query Protocol (VQP) client, which can query a VMPS such as a Catalyst 6500 series switch. The switch cannot be a VMPS servers. The VMPS server must be configured before a port is configured as dynamic.
- Use dynamic-access ports only to connect end stations. Connecting them to switches or routers (that use bridging protocols) can cause a loss of connectivity.
- Dynamic-access ports can only be in one VLAN and do not use VLAN tagging.
- Dynamic-access ports cannot be configured as:
  - Members of an EtherChannel port group (dynamic-access ports cannot be grouped with any other port, including other dynamic ports).
  - Source or destination ports in a static address entry.
  - Monitor ports.

## Examples

This example shows how to change a Layer 2 interface in access mode to operate in VLAN 2 instead of the default VLAN.

```
Switch(config-if)# switchport access vlan 2
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport mode** | Configures the VLAN membership mode of a port. |

# switchport block

Use the **switchport block** interface configuration command to prevent unknown multicast or unicast packets from being forwarded. Use the **no** form of this command to allow forwarding unknown multicast or unicast packets.

**switchport block** {**multicast | unicast**}

**no switchport block** {**multicast | unicast**}

## Syntax Description

| | |
|---|---|
| **multicast** | Specify that unknown multicast traffic should be blocked. |
| **unicast** | Specify that unknown unicast traffic should be blocked. |

## Defaults

Unknown multicast and unicast traffic is not blocked.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

By default, all traffic with unknown MAC addresses is sent to all ports. You can block unknown multicast or unicast traffic on protected or nonprotected ports. If unknown multicast or unicast traffic is not blocked on a protected port, there could be security issues.

If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport block** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

Blocking unknown multicast or unicast traffic is not automatically enabled on protected ports; you must explicitly configure it.

**Note** For more information about blocking packets, see the software configuration guide for this release.

## Examples

This example shows how to block unknown multicast traffic on an interface:

```
Switch(config-if)# switchport block multicast
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |

# switchport host

Use the **switchport host** interface configuration command to optimize a port for a host connection. The **no** form of this command has no affect on the system.

**switchport host**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The default is for the port to not be optimized for a host connection.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To optimize the port for a host connection, the **switchport host** command sets switch port mode to access, enables spanning tree Port Fast, and disables channel grouping. Only an end station can accept this configuration.

Because spanning tree Port Fast is enabled, you should enter the **switchport host** command only on ports that are connected to a single host. Connecting other switches, hubs, concentrators, or bridges to a fast-start port can cause temporary spanning-tree loops.

Enable the **switchport host** command to decrease the time that it takes to start up packet forwarding.

## Examples

This example shows how to optimize the port configuration for a host connection:

```
Switch(config-if)# switchport host
switchport mode will be set to access
spanning-tree portfast will be enabled
channel group will be disabled
Switch(config-if)#
```

You can verify your setting by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including switchport mode. |

# switchport mode

Use the **switchport mode** interface configuration command to configure the VLAN membership mode of a port. Use the **no** form of this command to reset the mode to the default.

**switchport mode** {**access** | **private-vlan** | **trunk**}

**no switchport mode**

## Syntax Description

| | |
|---|---|
| **access** | Set the port to access mode (either static-access or dynamic-access depending on the setting of the **switchport access vlan** interface configuration command). The port is set to access unconditionally and operates as a nontrunking, single VLAN interface that sends and receives unencapsulated (nontagged) frames. An access port can be assigned to only one VLAN. |
| **private-vlan** | See the **switchport mode private-vlan** command. |
| **trunk** | Set the port to trunk unconditionally. The port is a trunking VLAN Layer 2 interface. The port sends and receives encapsulated (tagged) frames that identify the VLAN of origination. A trunk is a point-to-point link between two switches or between a switch and a router. |

## Defaults

The default mode is **access**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A configuration that uses the **access** or **trunk** keywords takes effect only when you configure the port in the appropriate mode by using the **switchport mode** command. The static-access and trunk configuration are saved, but only one configuration is active at a time.

When you enter **access** mode, the interface changes to permanent nontrunking mode and negotiates to convert the link into a nontrunk link even if the neighboring interface does not agree to the change.

When you enter **trunk** mode, the interface changes to permanent trunking mode and negotiates to convert the link into a trunk link even if the interface connecting to it does not agree to the change. If you do not intend to trunk across those links, use the **switchport mode access** interface configuration command to disable trunking.

Access ports and trunk ports are mutually exclusive.

The IEEE 802.1x feature interacts with switchport modes in these ways:

- If you try to enable IEEE 802.1x on a trunk port, an error message appears, and IEEE 802.1x is not enabled. If you try to change the mode of an IEEE 802.1x-enabled port to trunk, the port mode is not changed.
- If you try to enable IEEE 802.1x on a dynamic-access (VLAN Query Protocol [VQP]) port, an error message appears, and IEEE 802.1x is not enabled. If you try to change an IEEE 802.1x-enabled port to dynamic VLAN assignment, an error message appears, and the VLAN configuration is not changed.

**Note** Only user network interfaces (UNIs) or enhanced network interfaces (ENIs) can be dynamic-access ports.

## Examples

This example shows how to configure a port for access mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode access
```

This example shows how to configure a port for trunk mode:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode trunk
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command and examining information in the Administrative Mode and Operational Mode rows.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport access vlan** | Configures a port as a static-access or dynamic-access port. |
| **switchport trunk** | Configures the trunk characteristics when an interface is in trunking mode. |

# switchport mode private-vlan

Use the **switchport mode private-vlan** interface configuration command to configure a port as a promiscuous or host private VLAN port. Use the **no switchport mode** command to reset the mode to the default access mode.

**switchport mode private-vlan** {**host** | **promiscuous**}

**no switchport mode private-vlan**

**Note** The **promiscuous** keyword is visible only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **host** | Configure the interface as a private-VLAN host port. Host ports belong to private-VLAN secondary VLANs and are either community ports or isolated ports, depending on the VLAN that they belong to. |
| **promiscuous** | Configure the interface as a private-VLAN promiscuous port. Promiscuous ports are members of private-VLAN primary VLANs. This keyword is only available on NNIs. User network interfaces (UNIs) or enhanced network interfaces (ENIs) cannot be configured as private VLAN promiscuous ports. |

## Defaults

The default private-VLAN mode is neither host nor promiscuous.

The default switchport mode is **access**.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A private-VLAN promiscuous port must be an NNI. To configure a UNI or an ENI as an NNI, enter the **port-type nni** interface configuration command.

A private-VLAN host or promiscuous port cannot be a Switched Port Analyzer (SPAN) destination port. If you configure a SPAN destination port as a private-VLAN host or promiscuous port, the port becomes inactive.

Do not configure private VLAN on ports with these other features:

- dynamic-access port VLAN membership
- Port Aggregation Protocol (PAgP) for only NNIs or ENIs
- Link Aggregation Control Protocol (LACP) only for NNIs or ENIs
- Multicast VLAN Registration (MVR)

A private-VLAN port cannot be a SPAN destination port.

While a port is part of the private-VLAN configuration, any EtherChannel configuration for it is inactive.

A private-VLAN port cannot be a secure port and should not be configured as a protected port.

**Note** For more information about private-VLAN interaction with other features, see the software configuration guide for this release.

If the port has STP enabled, we strongly recommend that you enable spanning tree Port Fast and bridge-protocol-data-unit (BPDU) guard on isolated and community host ports to prevent STP loops due to misconfigurations and to speed up STP convergence.

If you configure a port as a private-VLAN host port and you do not configure a valid private-VLAN association by using the **switchport private-vlan host-association** interface configuration command, the interface becomes inactive.

If you configure an NNI as a private-VLAN promiscuous port and you do not configure a valid private VLAN mapping by using the **switchport private-vlan mapping** interface configuration command, the interface becomes inactive.

## Examples

This example shows how to configure an interface as a private-VLAN host port and associate it to primary VLAN 20. The interface is a member of secondary isolated VLAN 501 and primary VLAN 20.

**Note** When you configure an NNI as a private VLAN host port, you should also enable BPDU guard and Port Fast by using the **spanning-tree portfast bpduguard default** global configuration command and the **spanning-tree portfast** interface configuration command.

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 501-503
Switch(config-if)# end
```

You can verify private VLAN switchport mode by using the **show interfaces** *interface-id* **switchport** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **private-vlan** | Configures a VLAN as a community, isolated, or primary VLAN or associates a primary VLAN with secondary VLANs. |
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including private VLAN configuration. |
| **switchport private-vlan** | Configures private VLAN associations and mappings between primary and secondary VLANs on an interface. |

# switchport port-security

Use the **switchport port-security** interface configuration command without keywords to enable port security on the interface. Use the keywords to configure secure MAC addresses, sticky MAC address learning, a maximum number of secure MAC addresses, or the violation mode. Use the **no** form of this command to disable port security or to set the parameters to their default states.

**switchport port-security** [**mac-address** *mac-address* [**vlan access**] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum** *value* [**vlan access**]]

**no switchport port-security** [**mac-address** *mac-address* [**vlan access**] | **mac-address sticky** [*mac-address* | **vlan access**]] [**maximum** *value* [**vlan access**]]

**switchport port-security** [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

**no switchport port-security** [**aging**] [**violation** {**protect** | **restrict** | **shutdown**}]

## Syntax Description

| | |
|---|---|
| **aging** | (Optional) See the **switchport port-security aging** command. |
| **mac-address** *mac-address* | (Optional) Specify a secure MAC address for the interface by entering a 48-bit MAC address. You can add additional secure MAC addresses up to the maximum value configured. |
| **vlan** *vlan-id* | (Optional) On a trunk port only, specify the VLAN ID and the MAC address. If no VLAN ID is specified, the native VLAN is used. |
| **vlan access** | (Optional) On an access port only, specify the VLAN as an access VLAN. |
| **mac-address sticky** [*mac-address*] | (Optional) Enable the interface for *sticky learning* by entering only the **mac-address sticky** keywords. When sticky learning is enabled, the interface adds all secure MAC addresses that are dynamically learned to the running configuration and converts these addresses to sticky secure MAC addresses.<br>(Optional) Enter a *mac-address* to specify a sticky secure MAC address. |
| **maximum** *value* | (Optional) Set the maximum number of secure MAC addresses for the interface.The maximum number of secure MAC addresses that you can configure on a switch is set by the maximum number of available MAC addresses allowed in the system, approximately 2000. This number represents the total of available MAC addresses, including those used for other Layer 2 functions and any other secure MAC addresses configured on interfaces.<br>The default setting is 1. |
| **vlan** [*vlan-list*] | (Optional) For trunk ports, you can set the maximum number of secure MAC addresses on a VLAN. If the **vlan** keyword is not entered, the default value is used.<br>• **vlan**—set a per-VLAN maximum value.<br>• **vlan** *vlan-list*—set a per-VLAN maximum value on a range of VLANs separated by a hyphen or a series of VLANs separated by commas. For nonspecified VLANs, the per-VLAN maximum value is used. |

| | |
|---|---|
| **violation** | (Optional) Set the security violation mode or the action to be taken if port security is violated. The default is **shutdown**. |
| **protect** | Set the security violation protect mode. In this mode, when the number of port secure MAC addresses reaches the maximum limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses to drop below the maximum value or increase the number of maximum allowable addresses. You are not notified that a security violation has occurred.<br>**Note** We do not recommend configuring the protect mode on a trunk port. The protect mode disables learning when any VLAN reaches its maximum limit, even if the port has not reached its maximum limit. |
| **restrict** | Set the security violation restrict mode. In this mode, when the number of secure MAC addresses reaches the limit allowed on the port, packets with unknown source addresses are dropped until you remove a sufficient number of secure MAC addresses or increase the number of maximum allowable addresses. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. |
| **shutdown** | Set the security violation shutdown mode. In this mode, the interface is error-disabled when a violation occurs and the port LED turns off. An SNMP trap is sent, a syslog message is logged, and the violation counter increments. When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause psecure-violation** global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands. |

## Defaults

The default is to disable port security.

When port security is enabled and no keywords are entered, the default maximum number of secure MAC addresses is 1.

The default violation mode is **shutdown**.

Sticky learning is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

A secure port has the following limitations:

- A secure port can be an access port or a trunk port; it cannot be a dynamic access port.
- A secure port cannot be a protected port.
- A secure port cannot be a destination port for Switched Port Analyzer (SPAN).
- A secure port cannot belong to a Fast EtherChannel or Gigabit EtherChannel port group.
- When you enter a maximum secure address value for an interface, if the new value is greater than the previous value, the new value overrides the previously configured value. If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.
- The switch does not support port security aging of sticky secure MAC addresses.

A security violation occurs when the maximum number of secure MAC addresses are in the address table and a station whose MAC address is not in the address table attempts to access the interface or when a station whose MAC address is configured as a secure MAC address on another secure port attempts to access the interface.

When a secure port is in the error-disabled state, you can bring it out of this state by entering the **errdisable recovery cause** *psecure-violation* global configuration command, or you can manually re-enable it by entering the **shutdown** and **no shut down** interface configuration commands.

Setting a maximum number of addresses to one and configuring the MAC address of an attached device ensures that the device has the full bandwidth of the port.

When you enter a maximum secure address value for an interface, this occurs:

- If the new value is greater than the previous value, the new value overrides the previously configured value.
- If the new value is less than the previous value and the number of configured secure addresses on the interface exceeds the new value, the command is rejected.

Sticky secure MAC addresses have these characteristics:

- When you enable sticky learning on an interface by using the **switchport port-security mac-address sticky** interface configuration command, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses and adds all sticky secure MAC addresses to the running configuration.
- If you disable sticky learning by using the **no switchport port-security mac-address sticky** interface configuration command or the running configuration is removed, the sticky secure MAC addresses remain part of the running configuration but are removed from the address table. The addresses that were removed can be dynamically reconfigured and added to the address table as dynamic addresses.
- When you configure sticky secure MAC addresses by using the **switchport port-security mac-address sticky** *mac-address* interface configuration command, these addresses are added to the address table and the running configuration. If port security is disabled, the sticky secure MAC addresses remain in the running configuration.

- If you save the sticky secure MAC addresses in the configuration file, when the switch restarts or the interface shuts down, the interface does not need to relearn these addresses. If you do not save the sticky secure addresses, they are lost. If sticky learning is disabled, the sticky secure MAC addresses are converted to dynamic secure addresses and are removed from the running configuration.
- If you disable sticky learning and enter the **switchport port-security mac-address sticky** *mac-address* interface configuration command, an error message appears, and the sticky secure MAC address is not added to the running configuration.

## Examples

This example shows how to enable port security on a port and to set the maximum number of secure addresses to 5. The violation mode is the default, and no secure MAC addresses are configured.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
```

This example shows how to configure a secure MAC address and a VLAN ID on a port.

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security mac-address 1000.2000.3000 vlan 3
```

This example shows how to enable sticky learning and to enter two sticky secure MAC addresses on a port:

```
Switch(config)# interface gigabitethernet 0/2
Switch(config-if)# switchport port-security mac-address sticky
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.4141
Switch(config-if)# switchport port-security mac-address sticky 0000.0000.000f
```

You can verify your settings by using the **show port-security** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **clear port-security** | Deletes from the MAC address table a specific type of secure address or all the secure addresses on the switch or an interface. |
| **show port-security address** | Displays all the secure addresses configured on the switch. |
| **show port-security interface** *interface-id* | Displays port security configuration for the switch or for the specified interface. |

# switchport port-security aging

Use the **switchport port-security aging** interface configuration command to set the aging time and type for secure address entries or to change the aging behavior for secure addresses on a particular port. Use the **no** form of this command to disable port security aging or to set the parameters to their default states.

**switchport port-security aging** {**static** | **time** *time* | **type** {**absolute** | **inactivity**}}

**no switchport port-security aging** {**static** | **time** | **type**}

## Syntax Description

| | |
|---|---|
| **static** | Enable aging for statically configured secure addresses on this port. |
| **time** *time* | Specify the aging time for this port. The range is 0 to 1440 minutes. If the time is 0, aging is disabled for this port. |
| **type** | Set the aging type. |
| **absolute** | Set absolute aging type. All the secure addresses on this port age out exactly after the time *(*minutes) specified and are removed from the secure address list. |
| **inactivity** | Set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period. |

## Defaults

The port security aging feature is disabled. The default time is 0 minutes.

The default aging type is absolute.

The default static aging behavior is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To enable secure address aging for a particular port, set the aging time to a value other than 0 for that port. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **switchport port-security aging** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

To allow limited time access to particular secure addresses, set the aging type as **absolute**. When the aging time lapses, the secure addresses are deleted.

To allow continuous access to a limited number of secure addresses, set the aging type as **inactivity**. This removes the secure address when it become inactive, and other addresses can become secure.

To allow unlimited access to a secure address, configure it as a secure address, and disable aging for the statically configured secure address by using the **no switchport port-security aging static** interface configuration command.

## Examples

This example sets the aging time as 2 hours for absolute aging for all the secure addresses on the port.

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport port-security aging time 120
```

This example sets the aging time as 2 minutes for inactivity aging type with aging enabled for configured secure addresses on the port.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport port-security aging time 2
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)# switchport port-security aging static
```

This example shows how to disable aging for configured secure addresses.

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# no switchport port-security aging static
```

## Related Commands

| Command | Description |
|---|---|
| show port-security | Displays the port security settings defined for the port. |
| switchport port-security | Enables port security on a port, restricts the use of the port to a user-defined group of stations, and configures secure MAC addresses. |

# switchport private-vlan

Use the **switchport private-vlan** interface configuration command to define a private-VLAN association for an isolated or community port or a mapping for a promiscuous port. Use the **no** form of this command to remove the private-VLAN association or mapping from the port.

**switchport private-vlan** {**association** {**host** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*} | **host-association** *primary-vlan-id secondary-vlan-id* | **mapping** *primary-vlan-id* {**add** | **remove**} *secondary-vlan-list*}

**no switchport private-vlan** {**association** {**host** | **mapping**} | **host-association** | **mapping**

**Note** The mapping commands are supported only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **association** | Define a private-VLAN association for a port. |
| **host** | Define a private-VLAN association for a community or isolated host port. |
| *primary-vlan-id* | The VLAN ID of the private-VLAN primary VLAN. The range is from 2 to 1001 and 1006 to 4094. |
| *secondary-vlan-id* | The VLAN ID of the private-VLAN secondary (isolated or community) VLAN. The range is from 2 to 1001 and 1006 to 4094. |
| **mapping** | Define private-VLAN mapping for a promiscuous port. Only NNIs can be configured as promiscuous ports. This keyword is not supported on user network interfaces (UNIs) or enhanced network interfaces (ENIs). |
| **add** | Associate secondary VLANs to the primary VLAN. |
| **remove** | Clear the association between secondary VLANs and the primary VLAN. |
| *secondary-vlan-list* | One or more secondary (isolated or community) VLANs to be mapped to the primary VLAN. |
| **host-association** | Define a private-VLAN association for a community or isolated host port. |

## Defaults

The default is to have no private-VLAN association or mapping configured.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Private-VLAN association or mapping has no effect on the port unless the port has been configured as a private-VLAN host or promiscuous port by using the **switchport mode private-vlan** {**host** | **promiscuous**} interface configuration command.

A promiscuous port must be an NNI; UNIs or ENIs cannot be configured as promiscuous ports. To configure a port as a UNI, enter the **port-type uni** interface configuration command.

If the port is in private-VLAN host or promiscuous mode but the VLANs do not exist, the command is allowed, but the port is made inactive.

The *secondary_vlan_list* parameter cannot contain spaces. It can contain multiple comma-separated items. Each item can be a single private-VLAN ID or a hyphenated range of private-VLAN IDs. The list can contain one isolated VLAN and multiple community VLANs.

You can map a promiscuous port to only one primary VLAN. If you enter the **switchport private-vlan mapping** command on a promiscuous port that is already mapped to a primary and secondary VLAN, the primary VLAN mapping is overwritten.

You can add or remove secondary VLANs from promiscuous port private-VLAN mappings by using the **add** and **remove** keywords.

Entering the **switchport private-vlan association host** command has the same effect as entering the **switchport private-vlan host-association** interface configuration command.

Entering the **switchport private-vlan association mapping** command has the same effect as entering the **switchport private-vlan mapping** interface configuration command.

## Examples

This example shows how to configure an interface as a private VLAN host port and associate it with primary VLAN 20 and secondary VLAN 501:

```
Switch# configure terminal
Switch(config)# interface fastethernet 0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 20 501
Switch(config-if)# end
```

This example shows how to configure an NNI as a private-VLAN promiscuous port and map it to a private VLAN. The interface is a member of primary VLAN 20 and secondary VLANs 501 to 503 are mapped to it.

```
Switch# configure terminal
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 20 add 501-503
Switch(config-if)# end
```

You can verify private-VLAN mapping by using the **show interfaces private-vlan mapping** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces private-vlan mapping** | Displays private VLAN mapping information for **VLAN SVIs.?** |
| **show vlan private-vlan** | Displays all private VLAN relationships or types configured on the switch. |

# switchport protected

Use the **switchport protected** interface configuration command to isolate unicast, multicast, and broadcast traffic at Layer 2 from other protected ports on the same switch. Use the **no** form of this command to disable protection on the port.

**switchport protected**

**no switchport protected**

**Note** Protected ports are supported only on network node interfaces (NNIs).

## Syntax Description

This command has no arguments or keywords.

## Defaults

No protected port is defined. All ports are nonprotected.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The switchport protection feature is local to the switch; communication between protected ports on the same switch is possible only through a Layer 3 device. To prevent communication between protected ports on different switches, you must configure the protected ports for unique VLANs on each switch and configure a trunk link between the switches. A protected port is different from a secure port.

A protected port does not forward any traffic (unicast, multicast, or broadcast) to any other port that is also a protected port. Data traffic cannot be forwarded between protected ports at Layer 2; only control traffic, such as PIM packets, is forwarded because these packets are processed by the CPU and forwarded in software. All data traffic passing between protected ports must be forwarded through a Layer 3 device.

Port monitoring does not work if both the monitor and monitored ports are protected ports.

## Examples

This example shows how to enable a protected port on an interface:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport protected
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport block** | Prevents unknown multicast or unicast traffic on the interface. |

# switchport trunk

Use the **switchport trunk** interface configuration command to set the trunk characteristics when the interface is in trunking mode. Use the **no** form of this command to reset a trunking characteristic to the default.

**switchport trunk** {**allowed vlan** *vlan-list* | **native vlan** *vlan-id*}

**no switchport trunk** {**allowed vlan** | **native vlan**}

## Syntax Description

| | |
|---|---|
| **allowed vlan** *vlan-list* | Set the list of allowed VLANs that can receive and send traffic on this interface in tagged format when in trunking mode. See the following *vlan-list* format. The **none** keyword is not valid. The default is **all**. |
| **native vlan** *vlan-id* | Set the native VLAN for sending and receiving untagged traffic when the interface is in 802.1Q trunking mode. The range is 1 to 4094. |

The *vlan-list* format is **all** | **none** | [**add** | **remove** | **except**] *vlan-atom* [**,***vlan-atom...*] where:

- **all** specifies all VLANs from 1 to 4094. This keyword is not allowed on commands that do not permit all VLANs in the list to be set at the same time.
- **none** means an empty list. This keyword is not allowed on commands that require certain VLANs to be set or at least one VLAN to be set.
- **add** adds the defined list of VLANs to those currently set instead of replacing the list. Valid IDs are from 1 to 4094. You can add extended-range VLANs (VLAN IDs greater than 1005) to the allowed VLAN list.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **remove** removes the defined list of VLANs from those currently set instead of replacing the list. Valid IDs are from 1 to 4094; extended-range VLAN IDs are valid.

  Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- **except** lists the VLANs that should be calculated by inverting the defined list of VLANs. (VLANs are added except the ones specified.) Valid IDs are from 1 to 1005. Separate nonconsecutive VLAN IDs with a comma; use a hyphen to designate a range of IDs.
- *vlan-atom* is either a single VLAN number from 1 to 4094 or a continuous range of VLANs described by two VLAN numbers, the lesser one first, separated by a hyphen.

## Defaults

VLAN 1 is the default native VLAN ID on the port.

The default for all VLAN lists is to include all VLANs.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Native VLANs:

- All untagged traffic received on an IEEE 802.1Q trunk port is forwarded with the native VLAN configured for the port.
- If a packet has a VLAN ID that is the same as the sending-port native VLAN ID, the packet is sent without a tag; otherwise, the switch sends the packet with a tag.
- The **no** form of the **native vlan** command resets the native mode VLAN to the appropriate default VLAN for the device.

Allowed VLAN:

- To reduce the risk of spanning-tree loops or storms, you can disable VLAN 1 on any individual VLAN trunk port by removing VLAN 1 from the allowed list. When you remove VLAN 1 from a trunk port, the interface continues to send and receive management traffic, for example, Cisco Discovery Protocol (CDP), Port Aggregation Protocol (PAgP), Link Aggregation Control Protocol (LACP), Dynamic Trunking Protocol (DTP), and VLAN Trunking Protocol (VTP) in VLAN 1.
- The **no** form of the **allowed vlan** command resets the list to the default list, which allows all VLANs.

## Examples

This example shows how to configure VLAN 3 as the default for the port to send all untagged traffic:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk native vlan 3
```

This example shows how to add VLANs 1, 2, 5, and 6 to the allowed list:

```
Switch(config)# interface gigabitethernet0/2
Switch(config-if)# switchport trunk allowed vlan add 1,2,5,6
```

You can verify your settings by entering the **show interfaces** *interface-id* **switchport** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces switchport** | Displays the administrative and operational status of a switching port, including port blocking and port protection settings. |
| **switchport mode** | Configures the VLAN membership mode of a port. |

# system mtu

Use the **system mtu** global configuration command to set the maximum packet size or maximum transmission unit (MTU) size for Gigabit Ethernet ports or for Fast Ethernet (10/100) ports. Use the **no** form of this command to restore the global MTU value to its default value.

**system mtu** {*bytes* | **jumbo** *bytes* | **routing** *bytes*}

**no system mtu**

**Note** Though visible in the command line help, the **routing** keyword is not supported.

## Syntax Description

| | |
|---|---|
| *bytes* | Set the system MTU for ports that are set to 10 or 100 Mbps. The range is 1500 to 1998 bytes. This is the maximum MTU received at 10/100-Mbps Ethernet switch ports. |
| **jumbo** *bytes* | Set the system jumbo frame size (MTU) for Gigabit Ethernet ports. The range is 1500 to 9000 bytes. This is the maximum MTU received at the physical port for Gigabit Ethernet ports. |

## Defaults

The default MTU size for all ports is 1500 bytes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(25)SEG | The **system mtu** `bytes` range was changed to 1500 to 1998. |

## Usage Guidelines

**Note** When you use this command to change the system MTU or jumbo MTU size, you must reset the switch before the new configuration takes effect.The system MTU setting is saved in the switch environmental variable in NVRAM and becomes effective when the switch reloads. The MTU settings you enter with the **system mtu** and **system mtu jumbo** commands are not saved in the switch IOS configuration file, even if you enter the **copy running-config startup-config** privileged EXEC command. Therefore, if you use TFTP to configure a new switch by using a backup configuration file and want the system MTU to be other than the default, you must explicitly configure the **system mtu** and **system mtu jumbo** settings on the new switch and then reload the switch.

Gigabit Ethernet ports operating at 1000 Mbps are not affected by the **system mtu** command, and 10/100-Mbps ports are not affected by the **system mtu jumbo** command.

If you enter a value that is outside the range for the specific type of switch, the value is not accepted.

**Note** The switch does not support setting the MTU on a per-interface basis.

The size of frames that can be received by the switch CPU is limited to 1998 bytes, regardless of the value entered with the **system mtu** command. Although forwarded or routed frames are usually not received by the CPU, some packets (for example, control traffic, SNMP, Telnet, and routing protocols) are sent to the CPU.

Because the switch does not fragment packets, it drops switched packets larger than the packet size supported on the *egress* interface.

For example, if the **system mtu** value is 1998 bytes and the **system mtu jumbo** value is 5000 bytes, packets up to 5000 bytes can be received on interfaces operating at 1000 Mbps. However, although a packet larger than 1998 bytes can be received on an interface operating at 1000 Mbps, if its destination interface is operating at 10 or 100 Mbps, the packet is dropped.

## Examples

This example shows how to set the maximum packet size for Gigabit Ethernet ports to 1800 bytes:

```
Switch(config)# system mtu jumbo 1800
Switch(config)# exit
Switch# reload
```

You can verify your setting by entering the **show system mtu** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| show system mtu | Displays the packet size set for Fast Ethernet and Gigabit Ethernet ports. |

# table-map

Use the **table-map** global configuration command to create a quality of service (QoS) mapping and to enter table-map configuration mode. Table maps can be specified in policy-map class **set** commands or as mark down mappings for policers and are used to create and configure a mapping table for converting one packet-marking value to another. Use the **no** form of this command to delete the mapping table.

**table-map** *table-map-name*

**no table-map** *table-map-name*

## Syntax Description

| | |
|---|---|
| *class-map-name* | Name of the table map. |

## Defaults

No table maps are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Use this command to specify the name of the table map that you want to create or to modify and to enter table-map configuration mode.

You use the **table-map** command to create a mapping table, which is a type of conversion chart used for establishing a *to-from* relationship between packet-marking types or categories. For example, you can use a mapping table to establish a to-from relationship among these categories:

- class of service (CoS)
- precedence
- Differentiated Services Code Point (DSCP)

The switch supports a maximum of 256 unique table maps.

The maximum number of map statements within a table map is 64.

After you are in table-map configuration mode, these configuration commands are available:

- **default**: the default behavior for setting a value not found in the table map. The default can be specified as one of these:
  - *default value*—uses the table map default value. The range is from 0 to 63.
  - **copy**—sets the default behavior for a value not found in the table map to copy.
  - **ignore**—sets the default behavior for a value not found in the table map to ignore.
- **exit**: exits from QoS table-map configuration mode.
- **map**: the table map **from** *from_value and* **to** *to_value*. Both value ranges are from 0 to 63.
- **no**: deletes the table map or sets the default values.

You can specify table maps in **set** commands and use them as mark-down mapping for the policers in input policy maps.

You cannot use table maps in output policy maps.

## Examples

This example shows how to create a table map to map DSCP to CoS values, setting those DSCP values that are not mapped to a CoS value of 4:

```
Switch(config)# table-map dscp-to-cos
Switch(config-tablemap)# map from 1 to 1
Switch(config-tablemap)# map from 2 to 1
Switch(config-tablemap)# map from 3 to 1
Switch(config-tablemap)# map from 4 to 2
Switch(config-tablemap)# map from 5 to 2
Switch(config-tablemap)# map from 6 to 3
Switch(config-tablemap)# default 4
Switch(config-tablemap)# exit
```

You can verify your settings by entering the **show table map** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **class** | Defines a traffic classification match criteria for the specified class-map name. |
| **policy-map** | Creates or modifies a policy map that can be attached to multiple ports to specify a service policy. |
| **set cos** | Classifies IP traffic by setting a CoS, DSCP, IP-precedence, or QoS group value in the packet. |
| **show table-map** | Displays QoS table maps. |

# test cable-diagnostics tdr

Use the **test cable-diagnostics tdr** privileged EXEC command to run the Time Domain Reflector (TDR) feature on an interface.

**test cable-diagnostics tdr interface** *interface-id*

**Note** TDR is supported only on the copper Ethernet 10/100 or 10/100/100 ports on the Cisco ME switch.

## Syntax Description

| | |
|---|---|
| *interface-id* | Specify the interface on which to run TDR. |

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can use the TDR feature to diagnose and resolve cabling problems. TDR is supported only on copper Ethernet 10/100 or 10/100/1000 ports. It is not supported on small form-factor pluggable (SFP) module ports. For more information about TDR, see the software configuration guide for this release.

After you run TDR by using the **test cable-diagnostics tdr interface** *interface-id* command, use the **show cable-diagnostics tdr interface** *interface-id* privileged EXEC command to display the results.

## Examples

This example shows how to run TDR on an interface:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/2
TDR test started on interface Gi0/2
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

If you enter the **test cable-diagnostics tdr interface** *interface-id* command on an interface that has a link status of up and a speed of 10 or 100 Mbps, these messages appear:

```
Switch# test cable-diagnostics tdr interface gigabitethernet0/3
TDR test on Gi0/9 will affect link state and traffic
TDR test started on interface Gi0/3
A TDR test can take a few seconds to run on an interface
Use 'show cable-diagnostics tdr' to read the TDR results.
```

## Related Commands

| Command | Description |
|---|---|
| **show cable-diagnostics tdr** | Displays the TDR results. |

# traceroute mac

Use the **traceroute mac** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address.

**traceroute mac** [**interface** *interface-id*] {*source-mac-address*} **[interface** *interface-id*] {*destination-mac-address*} [**vlan** *vlan-id*] [**detail**]

**Note** Layer 2 traceroute is available only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | (Optional) Specify an interface on the source or destination switch. |
| **source-mac-address** | Specify the MAC address of the source switch in hexadecimal format. |
| *destination-mac-address* | Specify the MAC address of the destination switch in hexadecimal format. |
| **vlan** *vlan-id* | (Optional) Specify the VLAN on which to trace the Layer 2 path that the packets take from the source switch to the destination switch. Valid VLAN IDs are 1 to 4094. |
| **detail** | (Optional) Specify that detailed information appears. |

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

**Note** Layer 2 traceroute is available only on NNIs.

When the switch detects a device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

Layer 2 traceroute supports only unicast traffic. If you specify a multicast source or destination MAC address, the physical path is not identified, and an error message appears.

The **traceroute mac** command output shows the Layer 2 path when the specified source and destination addresses belong to the same VLAN. If you specify source and destination addresses that belong to different VLANs, the Layer 2 path is not identified, and an error message appears.

If the source or destination MAC address belongs to multiple VLANs, you must specify the VLAN to which both the source and destination MAC addresses belong. If the VLAN is not specified, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination MAC addresses:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows how to display the Layer 2 path by using the **detail** keyword:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201 detail
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
ME-3400-24TS / 2.2.6.6 :
        Gi0/2 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the interfaces on the source and destination switches:

```
Switch# traceroute mac interface fastethernet0/1 0000.0201.0601 interface fastethernet0/3
0000.0201.0201
Source 0000.0201.0601 found on con6[ME-3400-24TS] (2.2.6.6)
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Gi0/1
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed
```

This example shows the Layer 2 path when the switch is not connected to the source switch:

```
Switch# traceroute mac 0000.0201.0501 0000.0201.0201 detail
Source not directly connected, tracing source .....
Source 0000.0201.0501 found on con5[ME-3400-24TS] (2.2.5.5)
con5 / ME-3400-24TS/ 2.2.5.5 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows the Layer 2 path when the switch cannot find the destination port for the source MAC address:

```
Switch# traceroute mac 0000.0011.1111 0000.0201.0201
Error:Source Mac address not found.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the source and destination devices are in different VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0301.0201
Error:Source and destination macs are on different vlans.
Layer2 trace aborted.
```

This example shows the Layer 2 path when the destination MAC address is a multicast address:

```
Switch# traceroute mac 0000.0201.0601 0100.0201.0201
Invalid destination mac address
```

This example shows the Layer 2 path when source and destination switches belong to multiple VLANs:

```
Switch# traceroute mac 0000.0201.0601 0000.0201.0201
Error:Mac found on multiple vlans.
Layer2 trace aborted.
```

## Related Commands

| Command | Description |
|---|---|
| traceroute mac ip | Displays the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname. |

# traceroute mac ip

Use the **traceroute mac ip** privileged EXEC command to display the Layer 2 path taken by the packets from the specified source IP address or hostname to the specified destination IP address or hostname.

**traceroute mac ip** {*source-ip-address* | *source-hostname*} {*destination-ip-address* | *destination-hostname*} [**detail**]

**Note** Layer 2 traceroute is available only on network node interfaces (NNIs).

## Syntax Description

| | |
|---|---|
| **source-ip-address** | Specify the IP address of the source switch as a 32-bit quantity in dotted-decimal format. |
| *destination-ip-address* | Specify the IP address of the destination switch as a 32-bit quantity in dotted-decimal format. |
| *source-hostname* | Specify the IP hostname of the source switch. |
| *destination-hostname* | Specify the IP hostname of the destination switch. |
| **detail** | (Optional) Specify that detailed information appears. |

## Defaults

There is no default.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For Layer 2 traceroute to function properly, Cisco Discovery Protocol (CDP) must be enabled on all the switches in the network. Do not disable CDP.

**Note** Layer 2 traceroute is available only on network node interfaces (NNIs).

When the switch detects an device in the Layer 2 path that does not support Layer 2 traceroute, the switch continues to send Layer 2 trace queries and lets them time out.

The maximum number of hops identified in the path is ten.

The **traceroute mac ip** command output shows the Layer 2 path when the specified source and destination IP addresses are in the same subnet. When you specify the IP addresses, the switch uses Address Resolution Protocol (ARP) to associate the IP addresses with the corresponding MAC addresses and the VLAN IDs.

- If an ARP entry exists for the specified IP address, the switch uses the associated MAC address and identifies the physical path.
- If an ARP entry does not exist, the switch sends an ARP query and tries to resolve the IP address. The IP addresses must be in the same subnet. If the IP address is not resolved, the path is not identified, and an error message appears.

The Layer 2 traceroute feature is not supported when multiple devices are attached to one port through hubs (for example, multiple CDP neighbors are detected on a port). When more than one CDP neighbor is detected on a port, the Layer 2 path is not identified, and an error message appears.

This feature is not supported in Token Ring VLANs.

## Examples

This example shows how to display the Layer 2 path by specifying the source and destination IP addresses and by using the **detail** keyword:

```
Switch# traceroute mac ip 2.2.66.66 2.2.22.22 detail
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6[WS-C2950G-24-EI] (2.2.6.6)
con6 / ME-3400-24TS-/ 2.2.6.6 :
        Gi0/1 [auto, auto] => Gi0/3 [auto, auto]
con5 / WS-C2950G-24-EI / 2.2.5.5 :
        Fa0/3 [auto, auto] => Gi0/1 [auto, auto]
con1 / WS-C3550-12G / 2.2.1.1 :
        Gi0/1 [auto, auto] => Gi0/2 [auto, auto]
con2 / WS-C3550-24 / 2.2.2.2 :
        Gi0/2 [auto, auto] => Fa0/1 [auto, auto]
Destination 0000.0201.0201 found on con2[WS-C3550-24] (2.2.2.2)
Layer 2 trace completed.
```

This example shows how to display the Layer 2 path by specifying the source and destination hostnames:

```
Switch# traceroute mac ip con6 con2
Translating IP to mac .....
2.2.66.66 => 0000.0201.0601
2.2.22.22 => 0000.0201.0201

Source 0000.0201.0601 found on con6
con6 (2.2.6.6) :Gi0/1 => Gi0/3
con5                 (2.2.5.5        )  :    Gi0/3 => Gi0/1
con1                 (2.2.1.1        )  :    Gi0/1 => Gi0/2
con2                 (2.2.2.2        )  :    Gi0/2 => Fa0/1
Destination 0000.0201.0201 found on con2
Layer 2 trace completed
```

This example shows the Layer 2 path when ARP cannot associate the source IP address with the corresponding MAC address:

```
Switch# traceroute mac ip 2.2.66.66 2.2.77.77
Arp failed for destination 2.2.77.77.
Layer2 trace aborted.
```

## Related Commands

| Command | Description |
|---|---|
| traceroute mac | Displays the Layer 2 path taken by the packets from the specified source MAC address to the specified destination MAC address. |

# udld

Use the **udld** global configuration command to enable aggressive or normal mode in the UniDirectional Link Detection (UDLD) and to set the configurable message timer time. Use the **no** form of the command to disable aggressive or normal mode UDLD on all fiber-optic ports.

**udld** {**aggressive** | **enable** | **message time** *message-timer-interval*}

**no udld** {**aggressive** | **enable** | **message**}

## Syntax Description

| | |
|---|---|
| **aggressive** | Enable UDLD in aggressive mode on all fiber-optic interfaces. |
| **enable** | Enable UDLD in normal mode on all fiber-optic interfaces. |
| **message time** *message-timer-interval* | Configure the period of time between UDLD probe messages on ports that are in the advertisement phase and are determined to be bidirectional. The range is 7 to 90 seconds. |

## Defaults

UDLD is disabled on all interfaces.

The message timer is set at 60 seconds.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the "Understanding UDLD" section in the software configuration guide for this release.

If you change the message time between probe packets, you are making a trade-off between the detection speed and the CPU load. By decreasing the time, you can make the detection-response faster but increase the load on the CPU.

This command affects fiber-optic interfaces only. Use the **udld** interface configuration command to enable UDLD on other interface types.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally

- The **no udld port** interface configuration command followed by the **udld port** or **udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state

## Examples

This example shows how to enable UDLD on all fiber-optic interfaces:

```
Switch(config)# udld enable
```

You can verify your setting by entering the **show udld** privileged EXEC **command**.

## Related Commands

| Command | Description |
|---|---|
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld port** | Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command. |
| **udld reset** | Resets all interfaces shut down by UDLD and permits traffic to again pass through. |

# udld port

Use the **udld port** interface configuration command to enable the UniDirectional Link Detection (UDLD) on an individual interface or prevent a fiber-optic interface from being enabled by the **udld** global configuration command. Use the **no** form of this command to return to the **udld** global configuration command setting or to disable UDLD if entered for a nonfiber-optic port.

**udld port** [**aggressive**]

**no udld port** [**aggressive**]

## Syntax Description

| | |
|---|---|
| **aggressive** | Enable UDLD in aggressive mode on the specified interface. |

## Defaults

On fiber-optic interfaces, UDLD is not enabled, not in aggressive mode, and not disabled. For this reason, fiber-optic interfaces enable UDLD according to the state of the **udld enable** or **udld aggressive** global configuration command.

On nonfiber-optic interfaces, UDLD is disabled.

## Command Modes

Interface configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

A UDLD-capable port cannot detect a unidirectional link if it is connected to a UDLD-incapable port of another switch. If the port is a user network interface (UNI) or enhanced network interface (ENI), you must use the **no shutdown** interface configuration command to enable it before using the **udld port** command. UNIs and ENIs are disabled by default. Network node interfaces (NNIs) are enabled by default.

UDLD supports two modes of operation: normal (the default) and aggressive. In normal mode, UDLD detects unidirectional links due to misconnected interfaces on fiber-optic connections. In aggressive mode, UDLD also detects unidirectional links due to one-way traffic on fiber-optic and twisted-pair links and due to misconnected interfaces on fiber-optic links. For information about normal and aggressive modes, see the “Configuring UDLD” chapter in the software configuration guide for this release.

To enable UDLD in normal mode, use the **udld port** interface configuration command. To enable UDLD in aggressive mode, use the **udld port aggressive** interface configuration command.

Use the **no udld port** command on fiber-optic ports to return control of UDLD to the **udld enable** global configuration command or to disable UDLD on nonfiber-optic ports.

Use the **udld port aggressive** command on fiber-optic ports to override the setting of the **udld enable** or **udld aggressive** global configuration command. Use the **no** form on fiber-optic ports to remove this setting and to return control of UDLD enabling to the **udld** global configuration command or to disable UDLD on nonfiber-optic ports.

If the switch software detects a small form-factor pluggable (SFP) module change and the port changes from fiber optic to nonfiber optic or the reverse, all configurations are maintained.

You can use these commands to reset an interface shut down by UDLD:

- The **udld reset** privileged EXEC command to reset all interfaces shut down by UDLD
- The **shutdown** and **no shutdown** interface configuration commands
- The **no udld enable** global configuration command followed by the **udld** {**aggressive** | **enable**} global configuration command to re-enable UDLD globally
- The **no udld port** interface configuration command followed by the **udld port or udld port aggressive** interface configuration command to re-enable UDLD on the specified interface
- The **errdisable recovery cause udld** and **errdisable recovery interval** *interval* global configuration commands to automatically recover from the UDLD error-disabled state

## Examples

This example shows how to enable UDLD on an port:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# udld port
```

This example shows how to disable UDLD on a fiber-optic interface despite the setting of the **udld** global configuration command:

```
Switch(config)# interface gigabitethernet0/1
Switch(config-if)# no udld port
```

You can verify your settings by entering the **show running-config** or the **show udld** *interface* privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld** | Enables aggressive or normal mode in UDLD or sets the configurable message timer time. |
| **udld reset** | Resets all interfaces shut down by UDLD and permits traffic to again pass through. |

# udld reset

Use the **udld reset** privileged EXEC command to reset all interfaces disabled by the UniDirectional Link Detection (UDLD) and permit traffic to begin passing through them again (though other features, such as spanning tree and Port Aggregation Protocol (PAgP) still have their normal effects, if enabled).

**udld reset**

**Note** PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If the interface configuration is still enabled for UDLD, these ports begin to run UDLD again and are disabled for the same reason if the problem has not been corrected.

## Examples

This example shows how to reset all interfaces disabled by UDLD:

```
Switch# udld reset
1 ports shutdown by UDLD were reset.
```

You can verify your setting by entering the **show udld** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show running-config** | Displays the operating configuration. For syntax information, use this link to the Cisco IOS Release 12.2 Command Reference listing page: http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/prod_command_reference_list.html Select the **Cisco IOS Commands Master List, Release 12.2** to navigate to the command. |
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |
| **udld** | Enables aggressive or normal mode in UDLD or sets the configurable message timer time. |
| **udld port** | Enables UDLD on an individual interface or prevents a fiber-optic interface from being enabled by the **udld** global configuration command. |

# uni-vlan

Use the **uni-vlan** VLAN configuration command to configure the VLAN as a user network interface-enhanced network interface (UNI-ENI) community or isolated VLAN. UNIs and ENIs on a switch that are assigned to a community VLAN can exchange packets with one another; UNIs and ENIs in an isolated VLAN cannot exchange packets. Use the **no** form of this command to return the VLAN to the default UNI-ENI isolated VLAN.

**uni-vlan** {**community** | **isolated**}

**no uni-vlan**

## Syntax Description

| | |
|---|---|
| **community** | Designate the UNI-ENI VLAN as a community VLAN. |
| **isolated** | Designate the UNI-ENI VLAN as an isolated VLAN. |

## Defaults

The default VLAN configuration is UNI-ENI isolated VLAN.

## Command Modes

VLAN configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

In a UNI-ENI isolated VLAN, packets are not exchanged between UNIs or ENIs within the VLAN. Packets can be exchanged between UNIs or ENIs and network node interfaces (NNIs) in the same UNI isolated VLAN.

In a UNI-ENI community VLAN, packets can be exchanged between UNIs, between ENIs, or between UNIs and NNIs in the same community VLAN. However, there can be no more than a combined total of eight UNIs and ENIs in a UNI community VLAN.

**Note** Local switching takes place between ENIs and UNIs in the same community VLAN. Because you can enable spanning tree on ENIs, but not on UNIs, you should use caution when configuring ENIs and UNIs in the same community VLAN. UNIs are always in the forwarding state.

VLAN 1 is always a UNI-ENI isolated VLAN; you cannot configure VLAN 1 as a UNI-ENI community VLAN. The reserved VLANs, 1002 to 1005, are not Ethernet VLANs.

As with any other VLAN, you can statically assign ports to UNI-ENI VLANs by using the **switchport access vlan** *vlan-id* interface configuration command. Ports are also dynamically assigned to UNI-ENI VLANs.

The **uni-vlan** command does not take effect until you exit from VLAN configuration mode.

A UNI-ENI VLAN cannot be a Remote Switched Port Analyzer (RSPAN) VLAN.

A UNI-ENI VLAN cannot be a private VLAN.

To change a UNI-ENI isolated VLAN to an RSPAN VLAN or a private VLAN, enter the **rspan-vlan** or **private-vlan** VLAN configuration command. This overwrites the default isolated VLAN configuration. To change a UNI-ENI community VLAN to an RSPAN VLAN or a private VLAN, you must first enter the **no uni-vlan** VLAN configuration command to return to the default UNI-ENI isolated VLAN configuration before entering the **rspan-vlan** or **private-vlan** VLAN configuration command.

**Note** For more information about UNI-ENI VLANs and interaction with other features, see the software configuration guide for this release.

## Examples

This example show s how to change VLAN 20 from the default UNI-ENI isolated VLAN to a UNI-ENI community VLAN:

```
Switch# configure terminal
Switch(config)# vlan 20
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
```

You can verify your setting by entering the **show vlan uni-vlan** or **show vlan** *vlan-id* **uni-vlan [type]** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show interfaces status** | Displays the status of interfaces, including the VLANs to which they belong. |
| **show vlan uni-vlan** | Displays the UNI-ENI VLANs on the switch. |

# vlan

Use the **vlan** global configuration command with a VLAN ID to add a VLAN and to enter VLAN configuration mode. Use the **no** form of this command to delete the VLAN. Configuration information for normal-range VLANs (VLAN IDs 1 to 1005) is always saved in the VLAN database as well as in the switch running configuration file. Configuration information for extended-range VLANs (VLAN IDs greater than 1005), are saved only in the switch running configuration file. You can save configurations in the switch startup configuration file by entering the **copy running-config startup-config** privileged EXEC command.

**vlan** *vlan-id*

**no vlan** *vlan-id*

## Syntax Description

| | |
|---|---|
| *vlan-id* | ID of the VLAN to be added and configured. For *vlan-id*, the range is 1 to 4094. You can enter a single VLAN ID, a series of VLAN IDs separated by commas, or a range of VLAN IDs separated by hyphens. |

## Defaults

This command has no default settings.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Extended-range VLANs (VLAN IDs 1006 to 4094) are not added to the VLAN database, but all VLAN configurations are saved in the running configuration, and you can save them in the switch startup configuration file.

Entering the **vlan** command with a VLAN ID enables VLAN configuration mode. If you enter an invalid VLAN ID, you receive an error message and do not enter VLAN configuration mode.

When you enter the VLAN ID of an existing VLAN, you do not create a new VLAN, but you can modify VLAN parameters for that VLAN. The specified VLANs are added or modified when you exit VLAN configuration mode. Only the **shutdown** command (for VLANs 1 to 1005) takes effect immediately.

These configuration commands are available in VLAN configuration mode. The **no** form of each command returns the characteristic to its default state.

**Note** Although all commands are visible, the only VLAN configuration commands that are supported on extended-range VLANs are **mtu** *mtu-size*, **private-vlan**, **remote-span** and **uni-vlan**. For extended-range VLANs, all other characteristics must remain at the default state.

**Note** The switch supports only Ethernet VLANs. You can configure parameters for FDDI and Token Ring VLANs and view the results in the vlan.dat file, but these parameters are not used.

- **are** *are-number*: defines the maximum number of all-routes explorer (ARE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **backupcrf {enable | disable}**: specifies the backup CRF mode for TrCRF VLANs.
- **bridge** {*bridge-number*| **type**}: specifies the logical distributed source-routing bridge, the bridge that interconnects all logical rings having this VLAN as a parent VLAN in FDDI-NET, Token Ring-NET, and TrBRF VLANs. The range is 0 to 15. The default bridge number is 0.
- **exit**: applies changes, increments the VLAN database revision number (VLANs 1 to 1005 only), and exits VLAN configuration mode.
- **media**: defines the VLAN media type.
  - **ethernet** is Ethernet media type (the default).
  - **fddi** is FDDI media type.
  - **fd-net** is FDDI network entity title (NET) media type.
  - **tokenring** is Token Ring media type or TrCRF.
  - **tr-net** is Token Ring network entity title (NET) media type or TrBRF media type.
- **mtu** *mtu-size*: specifies the maximum transmission unit (MTU) (packet size in bytes). The range is 1500 to 18190. The default is 1500 bytes.
- **name** *vlan-name*: names the VLAN with an ASCII string from 1 to 32 characters that must be unique within the administrative domain. The default is *VLANxxxx* where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number.
- **no**: negates a command or returns it to the default setting.
- **parent** *parent-vlan-id*: specifies the parent VLAN of an existing FDDI, Token Ring, or TrCRF VLAN. The range is 0 to 1005. The default parent VLAN ID is 0 (no parent VLAN).
- **private-vlan**: configure the VLAN as a private VLAN community, isolated, or primary VLAN or configure the association between private-VLAN primary and secondary VLANs. See the **private-vlan** command for more information.
- **remote-span**: configure the VLAN as a Remote SPAN (RSPAN) VLAN. When the RSPAN feature is added to an existing VLAN, the VLAN is first deleted and is then recreated with the RSPAN feature. Any access ports are deactivated until the RSPAN feature is removed. Learning is disabled on the VLAN. See the **remote-span** command for more information.
- **ring** *ring-number*: defines the logical ring for an FDDI, Token Ring, or TrCRF VLAN. The range is 1 to 4095.
- **said** *said-value*: specifies the security association identifier (SAID) as documented in IEEE 802.10. The range is 1 to 4294967294, and the number must be unique within the administrative domain. The default value is 100000 plus the VLAN ID number.
- **shutdown**: shuts down VLAN switching on the VLAN. This command takes effect immediately. Other commands take effect when you exit VLAN configuration mode.
- **state**: specifies the VLAN state:
  - **active** means the VLAN is operational (the default).
  - **suspend** means the VLAN is suspended. Suspended VLANs do not pass packets.

- **ste** *ste-number*: defines the maximum number of spanning-tree explorer (STE) hops for TrCRF VLANs. The range is 0 to 13. The default is 7.
- **stp type**: defines the spanning-tree type for FDDI-NET, Token Ring-NET, or TrBRF VLANs.
  - **ieee** for IEEE Ethernet STP running source-route transparent (SRT) bridging.
  - **ibm** for IBM STP running source-route bridging (SRB).
  - **auto** for STP running a combination of source-route transparent bridging (IEEE) and source-route bridging (IBM).
- **tb-vlan1** *tb-vlan1-id* and **tb-vlan2** *tb-vlan2-id*: specifies the first and second VLAN to which this VLAN is translationally bridged. Translational VLANs translate FDDI or Token Ring to Ethernet, for example. The range is 0 to 1005. If no value is specified, 0 (no transitional bridging) is assumed.
- **uni-vlan** {**community** | **isolated**}: configures the VLAN as a user network interface-enhanced network interface (UNI-ENI) community or UNI-ENI isolated VLAN. UNIs on a switch that are assigned to a community VLAN can communicate with each other. If the UNI-ENI VLAN is isolated (the default), ports in the VLAN cannot communicate. See the **uni-vlan** command for more information.

## Examples

This example shows how to add an Ethernet VLAN with default media characteristics. The default includes a *vlan-name* of *VLANxxx*, where *xxxx* represents four numeric digits (including leading zeros) equal to the VLAN ID number. The default **media** option is **ethernet**; the **state** option is **active**. The default *said-value* variable is 100000 plus the VLAN ID; the *mtu-size* variable is 1500; the **stp-type** option is **ieee**. When you enter the **exit** VLAN configuration command, the VLAN is added if it did not already exist; otherwise, this command does has no affect.

This example shows how to create a new VLAN with all default characteristics and enter config-vlan mode:

```
Switch(config)# vlan 200
Switch(config-vlan)# exit
```

This example shows how to create a new extended-range VLAN, to enter VLAN configuration mode and configure the VLAN as a UNI-ENI community VLAN, and to save the new VLAN in the switch startup configuration file:

```
Switch(config)# vlan 2000
Switch(config-vlan)# uni-vlan community
Switch(config-vlan)# exit
Switch(config)# exit
Switch# copy running-config startup config
```

You can verify your setting by entering the **show vlan** privileged EXEC command.

## Related Commands

| Command | Description |
|---|---|
| **show vlan** | Displays the parameters for all configured VLANs or one VLAN (if the VLAN ID or name is specified). |

# vlan access-map

Use the **vlan access-map** global configuration command to create or modify a VLAN map entry for VLAN packet filtering. This entry changes the mode to the VLAN access-map configuration. Use the **no** form of this command to delete a VLAN map entry. Use the **vlan filter** interface configuration command to apply a VLAN map to one or more VLANs.

**vlan access-map** *name* [*number*]

**no vlan access-map** *name* [*number*]

## Syntax Description

| | |
|---|---|
| *name* | Name of the VLAN map. |
| *number* | (Optional) The sequence number of the map entry that you want to create or modify (0 to 65535). If you are creating a VLAN map and the sequence number is not specified, it is automatically assigned in increments of 10, starting from 10. This number is the sequence to insert to, or delete from, a VLAN access-map entry. |

## Defaults

There are no VLAN map entries and no VLAN maps applied to a VLAN.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

In global configuration mode, use this command to create or modify a VLAN map. This entry changes the mode to VLAN access-map configuration, where you can use the **match** access-map configuration command to specify the access lists for IP or non-IP traffic to match and use the **action** command to set whether a match causes the packet to be forwarded or dropped.

In VLAN access-map configuration mode, these commands are available:

- **action**: sets the action to be taken (forward or drop).
- **default**: sets a command to its defaults
- **exit**: exits from VLAN access-map configuration mode
- **match**: sets the values to match (IP address or MAC address).
- **no**: negates a command or set its defaults

When you do not specify an entry number (sequence number), it is added to the end of the map.

There can be only one VLAN map per VLAN and it is applied as packets are received by a VLAN.

You can use the **no vlan access-map** *name* [*number*] command with a sequence number to delete a single entry.

In global configuration mode, use the **vlan filter** interface configuration command to apply the map to one or more VLANs.

**Note** For more information about VLAN map entries, see the software configuration guide for this release.

## Examples

This example shows how to create a VLAN map named *vac1* and apply matching conditions and actions to it. If no other entries already exist in the map, this will be entry 10.

```
Switch(config)# vlan access-map vac1
Switch(config-access-map)# match ip address acl1
Switch(config-access-map)# action forward
```

This example shows how to delete VLAN map *vac1*:

```
Switch(config)# no vlan access-map vac1
```

## Related Commands

| Command | Description |
|---|---|
| **action** | Sets the action for the VLAN access map entry. |
| **match (access-map configuration)** | Sets the VLAN map to match packets against one or more access lists. |
| **show vlan access-map** | Displays information about a particular VLAN access map or all VLAN access maps. |
| **vlan filter** | Applies the VLAN access map to one or more VLANs. |

# vlan filter

Use the **vlan filter** global configuration command to apply a VLAN map to one or more VLANs. Use the **no** form of this command to remove the map.

**vlan filter** *mapname* **vlan-list** {*list* | **all**}

**no vlan filter** *mapname* **vlan-list** {*list* | **all**}

## Syntax Description

| | |
|---|---|
| *mapname* | Name of the VLAN map entry. |
| *list* | The list of one or more VLANs in the form tt, uu-vv, xx, yy-zz, where spaces around commas and dashes are optional. The range is 1 to 4094. |
| **all** | Remove the filter from all VLANs. |

## Defaults

There are no VLAN filters.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To avoid accidentally dropping too many packets and disabling connectivity in the middle of the configuration process, we recommend that you completely define the VLAN access map before applying it to a VLAN.

**Note** For more information about VLAN map entries, see the software configuration guide for this release.

## Examples

This example applies VLAN map entry *map1* to VLANs 20 and 30:

```
Switch(config)# vlan filter map1 vlan-list 20, 30
```

This example shows how to delete VLAN map entry *mac1* from VLAN 20:

```
Switch(config)# no vlan filter map1 vlan-list 20
```

You can verify your settings by entering the **show vlan filter** privileged EXEC command.

**Related Commands**

| Command | Description |
|---|---|
| **show vlan access-map** | Displays information about a particular VLAN access map or all VLAN access maps. |
| **show vlan filter** | Displays information about all VLAN filters or about a particular VLAN or VLAN access map. |
| **vlan access-map** | Creates a VLAN map entry for VLAN packet filtering. |

# vmps reconfirm (privileged EXEC)

Use the **vmps reconfirm** privileged EXEC command to immediately send VLAN Query Protocol (VQP) queries to reconfirm all dynamic VLAN assignments with the VLAN Membership Policy Server (VMPS).

**vmps reconfirm**

## Syntax Description

This command has no arguments or keywords.

## Defaults

No default is defined.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to immediately send VQP queries to the VMPS:

```
Switch# vmps reconfirm
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining the VMPS Action row of the Reconfirmation Status section. The **show vmps** command shows the result of the last time the assignments were reconfirmed either because the reconfirmation timer expired or because the **vmps reconfirm** command was entered.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |
| **vmps reconfirm (global configuration)** | Changes the reconfirmation interval for the VQP client. |

# vmps reconfirm (global configuration)

Use the **vmps reconfirm** global configuration command to change the reconfirmation interval for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps reconfirm** *interval*

**no vmps reconfirm**

## Syntax Description

| | |
|---|---|
| *interval* | Reconfirmation interval for VQP client queries to the VLAN Membership Policy Server (VMPS) to reconfirm dynamic VLAN assignments. The range is 1 to 120 minutes. |

## Defaults

The default reconfirmation interval is 60 minutes.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to set the VQP client to reconfirm dynamic VLAN entries every 20 minutes:

```
Switch(config)# vmps reconfirm 20
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Reconfirm Interval row.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |
| **vmps reconfirm (privileged EXEC)** | Sends VQP queries to reconfirm all dynamic VLAN assignments with the VMPS. |

# vmps retry

Use the **vmps retry** global configuration command to configure the per-server retry count for the VLAN Query Protocol (VQP) client. Use the **no** form of this command to return to the default setting.

**vmps retry** *count*

**no vmps retry**

## Syntax Description

| | |
|---|---|
| *count* | Number of attempts to contact the VLAN Membership Policy Server (VMPS) by the client before querying the next server in the list. The range is 1 to 10. |

## Defaults

The default retry count is 3.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to set the retry count to 7:

```
Switch(config)# vmps retry 7
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the Server Retry Count row.

## Related Commands

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |

# vmps server

Use the **vmps server** global configuration command to configure the primary VLAN Membership Policy Server (VMPS) and up to three secondary servers. Use the **no** form of this command to remove a VMPS server.

**vmps server** *ipaddress* [**primary**]

**no vmps server** [*ipaddress*]

## Syntax Description

| | |
|---|---|
| *ipaddress* | IP address or hostname of the primary or secondary VMPS servers. If you specify a hostname, the Domain Name System (DNS) server must be configured. |
| **primary** | (Optional) Decides whether primary or secondary VMPS servers are being configured. |

## Defaults

No primary or secondary VMPS servers are defined.

## Command Modes

Global configuration

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The first server entered is automatically selected as the primary server whether or not **primary** is entered. The first server address can be overridden by using **primary** in a subsequent command.

When using the **no** form without specifying the *ipaddress*, all configured servers are deleted. If you delete all servers when dynamic-access ports are present, the switch cannot forward packets from new sources on these ports because it cannot query the VMPS.

## Examples

This example shows how to configure the server that has IP address 191.10.49.20 as the primary VMPS server. The servers with IP addresses 191.10.49.21 and 191.10.49.22 are configured as secondary servers:

```
Switch(config)# vmps server 191.10.49.20 primary
Switch(config)# vmps server 191.10.49.21
Switch(config)# vmps server 191.10.49.22
```

This example shows how to delete the server with IP address 191.10.49.21:

```
Switch(config)# no vmps server 191.10.49.21
```

You can verify your setting by entering the **show vmps** privileged EXEC command and examining information in the VMPS Domain Server row.

**Related Commands**

| Command | Description |
|---|---|
| **show vmps** | Displays VQP and VMPS information. |

APPENDIX A

# Cisco ME 2400 Ethernet Access Switch Boot Loader Commands

This appendix describes the boot loader commands on the Cisco ME 2400 Ethernet Access switch

During normal boot loader operation, you are not presented with the boot loader command-line prompt. You gain access to the boot loader command line if the switch is set to manually boot, if an error occurs during power-on self-test (POST) DRAM testing, or if an error occurs while loading the operating system (a corrupted Cisco IOS image). You can also access the boot loader if you have lost or forgotten the switch password.

**Note** The default switch configuration allows an end user with physical access to the switch to recover from a lost password by interrupting the boot process while the switch is powering up and then entering a new password. The password recovery disable feature allows the system administrator to protect access to the switch password by disabling part of this functionality and allowing the user to interrupt the boot process only by agreeing to set the system back to the default configuration. With password recovery disabled, the user can still interrupt the boot process and change the password, but the configuration file (config.text) and the VLAN database file (vlan.dat) are deleted. For more information, see the software configuration guide for this release.

You can access the boot loader through a switch console connection at 9600 bps. Disconnect and then reconnect the switch power cord. After the switch performs POST, the switch begins the autoboot process. The boot loader prompts the user for a break key character during the boot-up sequence, as shown in this example:

```
***** The system will autoboot in 15 seconds *****

Send a break key to prevent autobooting.
```

The break key character is different for each operating system.

- On a SUN work station running UNIX, Ctrl-C is the break key.
- On a PC running Windows 2000, Ctrl-Break is the break key.

Cisco TAC has tabulated break keys for most common operating systems and has provided an alternative break key sequence for terminal emulators that do not support the break keys. To view this table, see:

http://www.cisco.com/warp/public/701/61.html#how-to

When you enter the break key, the boot loader *switch:* prompt appears.

The boot loader performs low-level CPU initialization, performs POST, and loads a default operating system image into memory.

# boot

Use the **boot** boot loader command to load and boot an executable image and to enter the command-line interface.

**boot** [**-post** | **-n** | **-p** | *flag*] *filesystem***:/***file-url* ...

## Syntax Description

| | |
|---|---|
| **-post** | (Optional) Run the loaded image with an extended or comprehensive power-on self-test (POST). Using this keyword causes POST to take longer to complete. |
| -n | (Optional) Pause for the Cisco IOS debugger immediately after launching. |
| -p | (Optional) Pause for the JTAG debugger right after loading the image. |
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | (Optional) Path (directory) and name of a bootable image. Separate image names with a semicolon. |

## Defaults

The switch attempts to automatically boot the system by using information in the BOOT environment variable. If this variable is not set, the switch attempts to load and execute the first executable image it can by performing a recursive, depth-first search throughout the flash file system. In a depth-first search of a directory, each encountered subdirectory is completely searched before continuing the search in the original directory.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

When you enter the **boot** command without any arguments, the switch attempts to automatically boot the system by using the information in the BOOT environment variable, if any. If you supply an image name for the *file-url* variable, the **boot** command attempts to boot the specified image.

When you set boot loader **boot** command options, they are executed immediately and apply only to the current boot loader session. These settings are not saved for the next boot operation.

Filenames and directory names are case sensitive.

## Examples

This example shows how to boot the switch using the *new-image.bin* image:

```
switch: boot flash:/new-images/new-image.bin
```

After entering this command, you are prompted to start the setup program.

**Related Commands**

| Command | Description |
|---|---|
| set | Sets the BOOT environment variable to boot a specific image when the **BOOT** keyword is appended to the command. |

# cat

Use the **cat** boot loader command to display the contents of one or more files.

**cat** *filesystem***:***/file-url* ...

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | Path (directory) and name of the files to display. Separate each filename with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

## Examples

This example shows how to display the contents of two files:

```
switch: cat flash:/new-images/info flash:env_vars
version_suffix: metrobase-122-25.EX
version_directory: me240x-metrobase-mz.122-25.EX
image_name: me240x-metrobase-mz.122-25.EX.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: me340x
info_end:
BAUD=57600
MANUAL_BOOT=no
```

## Related Commands

| Command | Description |
|---|---|
| **more** | Displays the contents of one or more files. |
| **type** | Displays the contents of one or more files. |

# copy

Use the **copy** boot loader command to copy a file from a source to a destination.

**copy** [**-b** *block-size*] *filesystem***:/***source-file-url filesystem***:/***destination-file-url*

## Syntax Description

| | |
|---|---|
| **-b** *block-size* | (Optional) This option is used only for internal development and testing. |
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| **/***source-file-url* | Path (directory) and filename (source) to be copied. |
| **/***destination-file-url* | Path (directory) and filename of the destination. |

## Defaults

The default block size is 4 KB.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

If you are copying a file to a new directory, the directory must already exist.

## Examples

This example show how to copy a file at the root:

```
switch: copy flash:test1.text flash:test4.text
.
File "flash:test1.text" successfully copied to "flash:test4.text"
```

You can verify that the file was copied by entering the **dir** *filesystem***:** boot loader command.

## Related Commands

| Command | Description |
|---|---|
| **delete** | Deletes one or more files from the specified file system. |

# delete

Use the **delete** boot loader command to delete one or more files from the specified file system.

**delete** *filesystem***:**/*file-url* ...

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| /*file-url* | Path (directory) and filename to delete. Separate each filename with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

The switch prompts you for confirmation before deleting each file.

## Examples

This example shows how to delete two files:

```
switch: delete flash:test2.text flash:test5.text
Are you sure you want to delete "flash:test2.text" (y/n)?y
File "flash:test2.text" deleted
Are you sure you want to delete "flash:test5.text" (y/n)?y
File "flash:test2.text" deleted
```

You can verify that the files were deleted by entering the **dir flash:** boot loader command.

## Related Commands

| Command | Description |
|---|---|
| **copy** | Copies a file from a source to a destination. |

# dir

Use the **dir** boot loader command to display a list of files and directories on the specified file system.

**dir** *filesystem***:***/file-url ...*

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | (Optional) Path (directory) and directory name whose contents you want to display. Separate each directory name with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive.

## Examples

This example shows how to display the files in flash memory:

```
switch: dir flash:

Directory of flash:/

    3  -rwx        1839   Mar 01 2002 00:48:15  config.text
   11  -rwx        1140   Mar 01 2002 04:18:48  vlan.dat
   21  -rwx          26   Mar 01 2002 00:01:39  env_vars
    9  drwx         768   Mar 01 2002 23:11:42  html
   16  -rwx        1037   Mar 01 2002 00:01:11  config.text
   14  -rwx        1099   Mar 01 2002 01:14:05  homepage.htm
   22  -rwx          96   Mar 01 2002 00:01:39  system_env_vars
   17  drwx        192    Mar 06 2002 23:22:03  me240x-metrobase-mz.122-25.EX


15998976 bytes total (6397440 bytes free)
```

Table A-1 describes the fields in the display.

*Table A-1 dir Field Descriptions*

| Field | Description |
|---|---|
| 2 | Index number of the file. |
| -rwx | File permission, which can be any or all of the following:<br>• d—directory<br>• r—readable<br>• w—writable<br>• x—executable |
| 1644045 | Size of the file. |
| <date> | Last modification date. |
| env_vars | Filename. |

## Related Commands

| Command | Description |
|---|---|
| **mkdir** | Creates one or more directories. |
| **rmdir** | Removes one or more directories. |

# flash_init

Use the **flash_init** boot loader command to initialize the flash file system.

**flash_init**

## Syntax Description

This command has no arguments or keywords.

## Defaults

The flash file system is automatically initialized during normal system operation.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

During the normal boot process, the flash file system is automatically initialized.

Use this command to manually initialize the flash file system. For example, you use this command during the recovery procedure for a lost or forgotten password.

# format

Use the **format** boot loader command to format the specified file system and destroy all data in that file system.

**format** *filesystem***:**

**Syntax Description**

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

**Caution** Use this command with care; it destroys all data on the file system and renders your system unusable.

# fsck

Use the **fsck** boot loader command to check the file system for consistency.

**fsck** [**-test** | **-f**] *filesystem***:**

## Syntax Description

| | |
|---|---|
| **-test** | (Optional) Initialize the file system code and perform extra POST on flash memory. An extensive, nondestructive memory test is performed on every byte that makes up the file system. |
| **-f** | (Optional) Initialize the file system code and perform a fast file consistency check. Cyclic redundancy checks (CRCs) in the flashfs sectors are not checked. |
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |

## Defaults

No file system check is performed.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

To stop an in-progress file system consistency check, disconnect the switch power and then reconnect the power.

## Examples

This example shows how to perform an extensive file system check on flash memory:

```
switch: fsck -test flash:
```

# help

Use the **help** boot loader command to display the available commands.

**help**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You can also use the question mark (?) to display a list of available boot loader commands.

# memory

Use the **memory** boot loader command to display memory heap utilization information.

**memory**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to display memory heap utilization information:

```
switch: memory
Text:   0x00700000 - 0x0071cf24 (0x0001cf24 bytes)
Rotext: 0x00000000 - 0x00000000 (0x00000000 bytes)
Data:   0x0071cf24 - 0x00723a0c (0x00006ae8 bytes)
Bss:    0x0072529c - 0x00746f94 (0x00021cf8 bytes)
Heap:   0x00756f98 - 0x00800000 (0x000a9068 bytes)

Bottom heap utilization is 22 percent.
Top heap utilization is 0 percent.
Total heap utilization is 22 percent.
Total bytes: 0xa9068 (692328)
Bytes used: 0x26888 (157832)
Bytes available: 0x827e0 (534496)

Alternate heap utilization is 0 percent.
Total alternate heap bytes: 0x6fd000 (7327744)
Alternate heap bytes used: 0x0 (0)
Alternate heap bytes available: 0x6fd000 (7327744)
```

Table A-2 describes the fields in the display.

*Table A-2 memory Field Descriptions*

| Field | Description |
|---|---|
| Text | Beginning and ending address of the text storage area. |
| Rotext | Beginning and ending address of the read-only text storage area. This part of the data segment is grouped with the Text entry. |
| Data | Beginning and ending address of the data segment storage area. |
| Bss | Beginning and ending address of the block started by symbol (Bss) storage area. It is initialized to zero. |
| Heap | Beginning and ending address of the area in memory that memory is dynamically allocated to and freed from. |

# mkdir

Use the **mkdir** boot loader command to create one or more new directories on the specified file system.

**mkdir** *filesystem***:/***directory-url ...*

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */directory-url* | Name of the directories to create. Separate each directory name with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

## Examples

This example shows how to make a directory called Saved_Configs:

```
switch: mkdir flash:Saved_Configs
Directory "flash:Saved_Configs" created
```

This example shows how to make two directories:

```
switch: mkdir flash:Saved_Configs1 flash:Test
Directory "flash:Saved_Configs1" created
Directory "flash:Test" created
```

You can verify that the directory was created by entering the **dir** *filesystem***:** boot loader command.

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays a list of files and directories on the specified file system. |
| **rmdir** | Removes one or more directories from the specified file system. |

# more

Use the **more** boot loader command to display the contents of one or more files.

**more** *filesystem***:***/file-url ...*

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | Path (directory) and name of the files to display. Separate each filename with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

## Examples

This example shows how to display the contents of two files:

```
switch: more flash:/new-images/info flash:env_vars
version_suffix: metrobase-122-25.EX
version_directory: me240x-metrbase-mz.122-25.EX
image_name: me240x-metrobase-mz.122-25.EX.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: ME240x
info_end:
BAUD=57600
MANUAL_BOOT=no
```

## Related Commands

| Command | Description |
|---|---|
| **cat** | Displays the contents of one or more files. |
| **type** | Displays the contents of one or more files. |

# rename

Use the **rename** boot loader command to rename a file.

**rename** *filesystem*:*/source-file-url filesystem*:*/destination-file-url*

## Syntax Description

| | |
|---|---|
| *filesystem*: | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */source-file-url* | Original path (directory) and filename. |
| */destination-file-url* | New path (directory) and filename. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

Directory names are limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Filenames are limited to 45 characters; the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

## Examples

This example shows a file named *config.text* being renamed to *config1.text*:

```
switch: rename flash:config.text flash:config1.text
```

You can verify that the file was renamed by entering the **dir** *filesystem*: boot loader command.

## Related Commands

| Command | Description |
|---|---|
| copy | Copies a file from a source to a destination. |

# reset

Use the **reset** boot loader command to perform a hard reset on the system. A hard reset is similar to power-cycling the switch, clearing the processor, registers, and memory.

**reset**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to reset the system:

```
switch: reset
Are you sure you want to reset the system (y/n)?y
System resetting...
```

## Related Commands

| Command | Description |
|---|---|
| boot | Loads and boots an executable image and enters the command-line interface. |

# rmdir

Use the **rmdir** boot loader command to remove one or more empty directories from the specified file system.

**rmdir** *filesystem***:/***directory-url* ...

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */directory-url* | Path (directory) and name of the empty directories to remove. Separate each directory name with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Directory names are case sensitive and limited to 45 characters between the slashes (/); the name cannot contain control characters, spaces, deletes, slashes, quotes, semicolons, or colons.

Before removing a directory, you must first delete all the files in the directory.

The switch prompts you for confirmation before deleting each directory.

## Examples

This example shows how to remove a directory:

```
switch: rmdir flash:Test
```

You can verify that the directory was deleted by entering the **dir** *filesystem***:** boot loader command.

## Related Commands

| Command | Description |
|---|---|
| **dir** | Displays a list of files and directories on the specified file system. |
| **mkdir** | Creates one or more new directories on the specified file system. |

# set

Use the **set** boot loader command to set or display environment variables, which can be used to control the boot loader or any other software running on the switch.

**set** *variable value*

**Note** Under normal circumstances, it is not necessary to alter the setting of the environment variables.

**Syntax Description**

*variable value* Use one of these keywords for *variable and value*:

**MANUAL_BOOT**—Decides whether the switch automatically or manually boots.

Valid values are 1, yes, 0, and no. If it is set to no or 0, the boot loader attempts to automatically boot the system. If it is set to anything else, you must manually boot the switch from the boot loader mode.

**BOOT** *filesystem***:/***file-url*—A semicolon-separated list of executable files to try to load and execute when automatically booting.

If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash: file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.

**ENABLE_BREAK**—Decides whether the automatic boot process can be interrupted by using the Break key on the console.

Valid values are 1, yes, on, 0, no, and off. If it is set to 1, yes, or on, you can interrupt the automatic boot process by pressing the Break key on the console after the flash file system has initialized.

**HELPER** *filesystem***:/***file-url*—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.

**PS1** *prompt*—A string that is used as the command-line prompt in boot loader mode.

**CONFIG_FILE flash:/***file-url*—The filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.

**BAUD** *rate*—The rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting. The range is from 0 to 4294967295 bps. Valid values are 50, 75, 110, 150, 300, 600, 1200, 1800, 2000, 2400, 3600, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 56000, 57600, 115200, and 128000.

The most commonly used values are 300, 1200, 2400, 9600, 19200, 57600, and 115200.

**HELPER_CONFIG_FILE** *filesystem***:/***file-url*—The name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing.

**Defaults**

The environment variables have these default values:

MANUAL_BOOT: No (0)

BOOT: Null string

ENABLE_BREAK: No (Off or 0) (the automatic boot process cannot be interrupted by pressing the Break key on the console).

HELPER: No default value (helper files are not automatically loaded).

PS1: switch:

CONFIG_FILE: config.text

BAUD: 9600 bps

HELPER_CONFIG_FILE: No default value (no helper configuration file is specified).

SWITCH_NUMBER: 1

SWITCH_PRIORITY: 1

**Note** Environment variables that have values are stored in the flash file system in various files. The format of these files is that each line contains an environment variable name and an equal sign followed by the value of the variable. A variable has no value if it is not listed in this file; it has a value if it is listed in the file even if the value is a null string. A variable that is set to a null string (for example, " ") is a variable with a value. Many environment variables are predefined and have default values.

**Command Modes**

Boot loader

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

Environment variables are case sensitive and must be entered as documented.

Environment variables that have values are stored in flash memory outside of the flash file system.

The MANUAL_BOOT environment variable can also be set by using the **boot manual** global configuration command.

The BOOT environment variable can also be set by using the **boot system** *filesystem***:/***file-url* global configuration command.

The ENABLE_BREAK environment variable can also be set by using the **boot enable-break** global configuration command.

The HELPER environment variable can also be set by using the **boot helper** *filesystem***:/***file-url* global configuration command.

The CONFIG_FILE environment variable can also be set by using the **boot config-file flash:/***file-url* global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

The HELPER_CONFIG_FILE environment variable can also be set by using the **boot helper-config-file** *filesystem***:/***file-url* global configuration command.

The boot loader prompt string (PS1) can be up to 120 printable characters except the equal sign (=).

## Examples

This example shows how to change the boot loader prompt:

```
switch: set PS1 loader:
loader:
```

You can verify your setting by using the **set** boot loader command.

## Related Commands

| Command | Description |
|---|---|
| **unset** | Resets one or more environment variables to its previous setting. |

# type

Use the **type** boot loader command to display the contents of one or more files.

**type** *filesystem***:***/file-url* ...

## Syntax Description

| | |
|---|---|
| *filesystem***:** | Alias for a flash file system. Use **flash:** for the system board flash device. |
| */file-url* | Path (directory) and name of the files to display. Separate each filename with a space. |

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

Filenames and directory names are case sensitive.

If you specify a list of files, the contents of each file appears sequentially.

## Examples

This example shows how to display the contents of two files:

```
switch: type flash:/new-images/info flash:env_vars
version_suffix: metrobase-122-25.EX
version_directory: me240x-metrobase-mz.122-25.EX
image_name: me240x-metrobase-mz.122-25.EX.bin
ios_image_file_size: 63984644
total_image_file_size: 8133632
image_feature: IP|LAYER_3|PLUS|MIN_DRAM_MEG=128
image_family: me240x
info_end:
BAUD=57600
MANUAL_BOOT=no
```

## Related Commands

| Command | Description |
|---|---|
| **cat** | Displays the contents of one or more files. |
| **more** | Displays the contents of one or more files. |

# unset

Use the **unset** boot loader command to reset one or more environment variables.

**unset** *variable ...*

**Note** Under normal circumstances, it is not necessary to alter the setting of the environment variables.

**Syntax Description**

| | |
|---|---|
| *variable* | Use one of these keywords for *variable*:<br>**MANUAL_BOOT**—Decides whether the switch automatically or manually boots.<br>**BOOT**—Resets the list of executable files to try to load and execute when automatically booting. If the BOOT environment variable is not set, the system attempts to load and execute the first executable image it can find by using a recursive, depth-first search through the flash file system. If the BOOT variable is set but the specified images cannot be loaded, the system attempts to boot the first bootable file that it can find in the flash file system.<br>**ENABLE_BREAK**—Decides whether the automatic boot process can be interrupted by using the Break key on the console after the flash file system has been initialized.<br>**HELPER**—A semicolon-separated list of loadable files to dynamically load during the boot loader initialization. Helper files extend or patch the functionality of the boot loader.<br>**PS1**—A string that is used as the command-line prompt in boot loader mode.<br>**CONFIG_FILE**—Resets the filename that Cisco IOS uses to read and write a nonvolatile copy of the system configuration.<br>**BAUD**—Resets the rate in bits per second (bps) used for the console. The Cisco IOS software inherits the baud rate setting from the boot loader and continues to use this value unless the configuration file specifies another setting.<br>**HELPER_CONFIG_FILE**—Resets the name of the configuration file to be used by the Cisco IOS helper image. If this is not set, the file specified by the CONFIG_FILE environment variable is used by all versions of Cisco IOS that are loaded, including the helper image. This variable is used only for internal development and testing. |

**Command Modes** Boot loader

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The MANUAL_BOOT environment variable can also be reset by using the **no boot manual** global configuration command.

The BOOT environment variable can also be reset by using the **no boot system** global configuration command.

The ENABLE_BREAK environment variable can also be reset by using the **no boot enable-break** global configuration command.

The HELPER environment variable can also be reset by using the **no boot helper** global configuration command.

The CONFIG_FILE environment variable can also be reset by using the **no boot config-file** global configuration command.

The HELPER_CONFIG_FILE environment variable can also be reset by using the **no boot helper-config-file** global configuration command.

## Examples

This example shows how to reset the prompt string to its previous setting:

```
switch: unset PS1
switch:
```

## Related Commands

| Command | Description |
|---|---|
| **set** | Sets or displays environment variables. |

# version

Use the **version** boot loader command to display the boot loader version.

**version**

## Syntax Description

This command has no arguments or keywords.

## Command Modes

Boot loader

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Examples

This example shows how to display the boot loader version:

```
switch: version
ME3400 Boot Loader (ME340x-HBOOT-M) Version 12.2(25)EX
Compiled Wed 12-Sept-05 14:58 by devgoyal

switch:
```

APPENDIX B

# Cisco ME 2400 Ethernet Access Switch Debug Commands

This appendix describes the **debug** privileged EXEC commands that have been created or changed for use with the Cisco ME 2400 Ethernet Access switch. These commands are helpful in diagnosing and resolving internetworking problems and should be enabled only under the guidance of Cisco technical support staff.

**Caution** Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use the **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with Cisco technical support staff. It is best to use the **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

# debug dot1x

Use the **debug dot1x** privileged EXEC command to enable debugging of the IEEE 802.1x feature. Use the **no** form of this command to disable debugging.

**debug dot1x** {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

**no debug dot1x** {**all** | **errors** | **events** | **packets** | **registry** | **state-machine**}

## Syntax Description

| | |
|---|---|
| **all** | Display all IEEE 802.1x debug messages. |
| **errors** | Display IEEE 802.1x error debug messages. |
| **events** | Display IEEE 802.1x event debug messages. |
| **packets** | Display IEEE 802.1x packet debug messages. |
| **registry** | Display IEEE 802.1x registry invocation debug messages. |
| **state-machine** | Display state-machine related-events debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug dot1x** command is the same as the **no debug dot1x** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show dot1x** | Displays IEEE 802.1x statistics, administrative status, and operational status for the switch or for the specified port. |

# debug etherchannel

Use the **debug etherchannel** privileged EXEC command to enable debugging of the EtherChannel/PAgP shim. This shim is the software module that is the interface between the Port Aggregation Protocol (PAgP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

**debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]

**no debug etherchannel** [**all** | **detail** | **error** | **event** | **idb**]

**Note** PAgP is available only on network node interfaces (NNIs) or enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all EtherChannel debug messages. |
| **detail** | (Optional) Display detailed EtherChannel debug messages. |
| **error** | (Optional) Display EtherChannel error debug messages. |
| **event** | (Optional) Debug major EtherChannel event messages. |
| **idb** | (Optional) Display PAgP interface descriptor block debug messages. |

**Note** Though visible in the command-line help strings, the **linecard** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug etherchannel** command is the same as the **no debug etherchannel** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show etherchannel** | Displays EtherChannel information for the channel. |

# debug interface

Use the **debug interface** privileged EXEC command to enable debugging of interface-related activities. Use the **no** form of this command to disable debugging.

**debug interface** {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

**no debug interface** {*interface-id* | **null** *interface-number* | **port-channel** *port-channel-number* | **vlan** *vlan-id*}

## Syntax Description

| | |
|---|---|
| *interface-id* | Display debug messages for the specified physical port, identified by type switch number/module number/ port, for example **gigabitethernet 0/2**. |
| **null** *interface-number* | Display debug messages for null interfaces. The *interface-number* is always **0**. |
| **port-channel** *port-channel-number* | Display debug messages for the specified EtherChannel port-channel interface. The *port-channel-number* range is 1 to 48. |
| **vlan** *vlan-id* | Display debug messages for the specified VLAN. The *vlan-id* range is 1 to 4094. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a keyword, all debug messages appear.

The **undebug interface** command is the same as the **no debug interface** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show etherchannel** | Displays EtherChannel information for the channel. |

# debug ip igmp filter

Use the **debug ip igmp filter** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) filter events. Use the **no** form of this command to disable debugging.

**debug ip igmp filter**

**no debug ip igmp filter**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug ip igmp filter** command is the same as the **no debug ip igmp filter** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug ip igmp max-groups

Use the **debug ip igmp max-groups** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) maximum groups events. Use the **no** form of this command to disable debugging.

**debug ip igmp max-groups**

**no debug ip igmp max-groups**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug ip igmp max-groups** command is the same as the **no debug ip igmp max-groups** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug ip igmp snooping

Use the **debug igmp snooping** privileged EXEC command to enable debugging of Internet Group Management Protocol (IGMP) snooping activity. Use the **no** form of this command to disable debugging.

**debug ip igmp snooping** [**group** | **management** | **querier** | **router** | **timer**]

**no debug ip igmp snooping** [**group** | **management** | **querier** | **router** | **timer**]

## Syntax Description

| | |
|---|---|
| **group** | (Optional) Display IGMP snooping group activity debug messages. |
| **management** | (Optional) Display IGMP snooping management activity debug messages. |
| **querier** | (Optional) Display IGMP snooping querier debug messages. |
| **router** | (Optional) Display IGMP snooping router activity debug messages. |
| **timer** | (Optional) Display IGMP snooping timer event debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug ip igmp snooping** command is the same as the **no debug ip igmp snooping** command.

## Related Commands

| Command | Description |
|---|---|
| **debug platform ip igmp snooping** | Displays information about platform-dependent IGMP snooping activity. |
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug lacp

Use the **debug lacp** privileged EXEC command to enable debugging of Link Aggregation Control Protocol (LACP) activity. Use the **no** form of this command to disable debugging.

**debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]

**no debug lacp** [**all** | **event** | **fsm** | **misc** | **packet**]

**Note** LACP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all LACP debug messages. |
| **event** | (Optional) Display LACP event debug messages. |
| **fsm** | (Optional) Display LACP finite state-machine debug messages. |
| **misc** | (Optional) Display miscellaneous LACP debug messages. |
| **packet** | (Optional) Display LACP packet debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug lacp** command is the same as the **no debug lacp** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show lacp** | Displays LACP channel-group information. |

# debug mac-notification

Use the **debug mac-notification** privileged EXEC command to enable debugging of MAC notification events. Use the **no** form of this command to disable debugging.

**debug mac-notification**

**no debug mac-notification**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug mac-notification** command is the same as the **no debug mac-notification** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show mac address-table notification** | Displays the MAC address notification information for all interfaces or the specified interface. |

# debug matm

Use the **debug matm** privileged EXEC command to enable debugging of platform-independent MAC address management. Use the **no** form of this command to disable debugging.

**debug matm**

**no debug matm**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug matm** command is the same as the **no debug matm** command.

## Related Commands

| Command | Description |
|---|---|
| **debug platform matm** | Displays information about platform-dependent MAC address management. |
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug monitor

Use the **debug monitor** privileged EXEC command to enable debugging of the Switched Port Analyzer (SPAN) feature. Use the **no** form of this command to disable debugging.

**debug monitor** {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

**no debug monitor** {**all** | **errors** | **idb-update** | **info** | **list** | **notifications** | **platform** | **requests** | **snmp**}

## Syntax Description

| | |
|---|---|
| **all** | Display all SPAN debug messages. |
| **errors** | Display detailed SPAN error debug messages. |
| **idb-update** | Display SPAN interface description block (IDB) update-trace debug messages. |
| **info** | Display SPAN informational-tracing debug messages. |
| **list** | Display SPAN port and VLAN-list tracing debug messages. |
| **notifications** | Display SPAN notification debug messages. |
| **platform** | Display SPAN platform-tracing debug messages. |
| **requests** | Display SPAN request debug messages. |
| **snmp** | Display SPAN and Simple Network Management Protocol (SNMP) tracing debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug monitor** command is the same as the **no debug monitor** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show monitor** | Displays information about all SPAN and remote SPAN (RSPAN) sessions on the switch. |

# debug mvrdbg

Use the **debug mvrdbg** privileged EXEC command to enable debugging of Multicast VLAN Registration (MVR). Use the **no** form of this command to disable debugging.

**debug mvrdbg** {**all** | **events** | **igmpsn** | **management** | **ports**}

**no debug mvrdbg** {**all** | **events** | **igmpsn** | **management** | **ports**}

## Syntax Description

| | |
|---|---|
| **all** | Display all MVR activity debug messages. |
| **events** | Display MVR event-handling debug messages. |
| **igmpsn** | Display MVR Internet Group Management Protocol (IGMP) snooping-activity debug messages. |
| **management** | Display MVR management-activity debug messages. |
| **ports** | Display MVR port debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug mvrdbg** command is the same as the **no debug mvrdbg** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show mvr** | Displays the current MVR configuration. |

# debug nvram

Use the **debug nvram** privileged EXEC command to enable debugging of NVRAM activity. Use the **no** form of this command to disable debugging.

**debug nvram**

**no debug nvram**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug nvram** command is the same as the **no debug nvram** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug pagp

Use the **debug pagp** privileged EXEC command to enable debugging of Port Aggregation Protocol (PAgP) activity. Use the **no** form of this command to disable debugging.

**debug pagp** [**all** | **event** | **fsm** | **misc** | **packet**]

**no debug pagp** [**all** | **event** | **fsm** | **misc** | **packet**]

**Note** PAgP is available only on network node interfaces (NNIs) and enhanced network interfaces (ENIs).

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all PAgP debug messages. |
| **event** | (Optional) Display PAgP event debug messages. |
| **fsm** | (Optional) Display PAgP finite state-machine debug messages. |
| **misc** | (Optional) Display miscellaneous PAgP debug messages. |
| **packet** | (Optional) Display PAgP packet debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug pagp** command is the same as the **no debug pagp** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show pagp** | Displays PAgP channel-group information. |

# debug platform acl

Use the **debug platform acl** privileged EXEC command to enable debugging of the access control list (ACL) manager. Use the **no** form of this command to disable debugging.

**debug platform acl** {**all** | **exit** | **label** | **main** | **vacl** | **vlmap** | **warn**}

**no debug platform acl** {**all** | **exit** | **label** | **main** | **vacl** | **vlmap** | **warn**}

## Syntax Description

| | |
|---|---|
| **all** | Display all ACL manager debug messages. |
| **exit** | Display ACL exit-related debug messages. |
| **label** | Display ACL label-related debug messages. |
| **main** | Display the main or important ACL debug messages. |
| **vacl** | Display VLAN ACL-related debug messages. |
| **vlmap** | Display ACL VLAN-map-related debug messages. |
| **warn** | Display ACL warning-related debug messages. |

**Note** Though visible in the command-line help strings, the **racl** and **stack** keywords are not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform acl** command is the same as the **no debug platform acl** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform cpu-queues

Use the **debug platform cpu-queues** privileged EXEC command to enable debugging of platform central processing unit (CPU) receive queues. Use the **no** form of this command to disable debugging.

**debug platform cpu-queues** {**broadcast-q** | **cbt-to-spt-q** | **cpuhub-q** | **host-q** | **icmp-q** | **igmp-snooping-q** | **layer2-protocol-q** | **logging-q** | **remote-console-q** | **software-fwd-q** | **stp-q**}

**no debug platform cpu-queues** {**broadcast-q** | **cbt-to-spt-q** | **cpuhub-q** | **host-q** | **icmp-q** | **igmp-snooping-q** | **layer2-protocol-q** | **logging-q** | **remote-console-q** | **software-fwd-q** | **stp-q**}

## Syntax Description

| | |
|---|---|
| **broadcast-q** | Display debug messages about packets received by the broadcast queue. |
| **cbt-to-spt-q** | Display debug messages about packets received by the core-based tree to shortest-path tree (cbt-to-spt) queue. |
| **cpuhub-q** | Display debug messages about packets received by the CPU heartbeat queue. |
| **host-q** | Display debug messages about packets received by the host queue. |
| **icmp-q** | Display debug messages about packets received by the Internet Control Message Protocol (ICMP) queue. |
| **igmp-snooping-q** | Display debug messages about packets received by the Internet Group Management Protocol (IGMP)-snooping queue. |
| **layer2-protocol-q** | Display debug messages about packets received by the Layer 2 protocol queue. |
| **logging-q** | Display debug messages about packets received by the logging queue. |
| **remote-console-q** | Display debug messages about packets received by the remote console queue. |
| **software-fwd-q** | Debug packets received by the software forwarding queue. |
| **stp-q** | Debug packets received by the Spanning Tree Protocol (STP) queue. |

**Note** Though visible in the command-line help strings, the **routing-protocol-Q** and **rpffail-q** keywords are not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform cpu-queues** command is the same as the **no debug platform cpu-queues** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform dot1x

Use the **debug platform dot1x** privileged EXEC command to enable debugging of IEEE 802.1x events. Use the **no** form of this command to disable debugging.

**debug platform dot1x** {**initialization** | **interface-configuration** | **rpc**}

**no debug platform dot1x** {**initialization** | **interface-configuration** | **rpc**}

## Syntax Description

| | |
|---|---|
| **initialization** | Display IEEE 802.1x initialization sequence debug messages. |
| **interface-configuration** | Display IEEE 802.1x interface configuration-related debug messages. |
| **rpc** | Display IEEE 802.1x remote procedure call (RPC) request debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform dot1x** command is the same as the **no debug platform dot1x** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform etherchannel

Use the **debug platform etherchannel** privileged EXEC command to enable debugging of platform-dependent EtherChannel events. Use the **no** form of this command to disable debugging.

**debug platform etherchannel** {**init** | **link-up** | **rpc-detailed** | **rpc-generic** | **warnings**}

**no debug platform etherchannel** {**init** | **link-up** | **rpc-detailed** | **rpc-generic** | **warnings**}

## Syntax Description

| | |
|---|---|
| **init** | Display EtherChannel module initialization debug messages. |
| **link-up** | Display EtherChannel link-up and link-down related debug messages. |
| **rpc-detailed** | Display detailed EtherChannel remote procedure call (RPC) debug messages. |
| **rpc-generic** | Display EtherChannel RPC generic debug messages. |
| **warnings** | Display EtherChannel warning debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform etherchannel** command is the same as the **no debug platform etherchannel** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform forw-tcam

Use the **debug platform forw-tcam** privileged EXEC command to enable debugging of the forwarding ternary content addressable memory (TCAM) manager. Use the **no** form of this command to disable debugging.

**debug platform forw-tcam** [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

**no debug platform forw-tcam** [**adjustment** | **allocate** | **audit** | **error** | **move** | **read** | **write**]

## Syntax Description

| | |
|---|---|
| **adjustment** | (Optional) Display TCAM manager adjustment debug messages. |
| **allocate** | (Optional) Display TCAM manager allocation debug messages. |
| **audit** | (Optional) Display TCAM manager audit messages. |
| **error** | (Optional) Display TCAM manager error messages. |
| **move** | (Optional) Display TCAM manager move messages. |
| **read** | (Optional) Display TCAM manager read messages. |
| **write** | (Optional) Display TCAM manager write messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

If you do not specify a keyword, all forwarding TCAM manager debug messages appear.

The **undebug platform forw-tcam** command is the same as the **no debug platform forw-tcam** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform ip dhcp

Use the **debug platform ip dhcp** privileged EXEC command to debug DHCP events. Use the **no** form of this command to disable debugging.

**debug platform ip dhcp** [**all** | **error** | **event** | **packet** | **rpc**]

**no debug platform ip dhcp** [**all** | **error** | **event** | **packet** | **rpc**]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all DHCP debug messages. |
| **error** | (Optional) Display DHCP error debug messages. |
| **event** | (Optional) Display DHCP event debug messages. |
| **packet** | (Optional) Display DHCP packet-related debug messages. |
| **rpc** | (Optional) Display DHCP remote procedure call (RPC) request debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform ip dhcp** command is the same as the **no debug platform ip dhcp** command.

## Related Commands

| Command | Description |
|---|---|
| **show ip dhcp snooping** | Displays the DHCP snooping configuration. |
| **show ip dhcp snooping binding** | Displays the DHCP snooping binding information. |
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform ip igmp snooping

Use the **debug platform ip igmp snooping** privileged EXEC command to enable debugging of platform-dependent Internet Group Management Protocol (IGMP) snooping. Use the **no** form of this command to disable debugging.

**debug platform ip igmp snooping** {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

**debug platform ip igmp snooping pak** {*ip-address* | **error** | **ipopt** | **leave**| **query** | **report** | **rx** | **svi** | **tx**}

**debug platform ip igmp snooping rpc** [**cfg** | **misc** | **vlan**]

**no debug platform ip igmp snooping** {**all** | **di** | **error** | **event** | **group** | **mgmt** | **pak** | **retry** | **rpc** | **warn**}

## Syntax Description

| | |
|---|---|
| **all** | Display all IGMP snooping debug messages. |
| **di** | Display IGMP snooping destination index (di) coordination remote procedure call (RPC) debug messages. |
| **error** | Display IGMP snooping error messages. |
| **event** | Display IGMP snooping event debug messages. |
| **group** | Display IGMP snooping group debug messages. |
| **mgmt** | Display IGMP snooping management debug messages. |
| **pak** {*ip-address* \| **error** \| **ipopt** \| **leave** \| **query** \| **report** \| **rx** \| **svi** \| **tx**} | Display IGMP snooping packet event debug messages. The keywords have these meanings:<br>• *ip-address*—IP address of the IGMP group.<br>• **error**—Display IGMP snooping packet error debug messages.<br>• **ipopt**—Display IGMP snooping IP bridging options debug messages.<br>• **leave**—Display IGMP snooping leave debug messages.<br>• **query**—Display IGMP snooping query debug messages.<br>• **report**—Display IGMP snooping report debug messages.<br>• **rx**—Display IGMP snooping received packet debug messages.<br>• **svi**—Display IGMP snooping switched virtual interface (SVI) packet debug messages.<br>• **tx**—Display IGMP snooping sent packet debug messages. |
| **private-vlan** | Display IGMP snooping private VLAN messages. |
| **retry** | Display IGMP snooping retry debug messages. |
| **rpc** [**cfg** \| **misc** \| **vlan**] | Display IGMP snooping remote procedure call (RPC) event debug messages. The keywords have these meanings:<br>• **cfg**—(Optional) Display IGMP snooping RPC debug messages.<br>• **misc**—(Optional) IGMP snooping miscellaneous RPC debug messages.<br>• **vlan**—(Optional) IGMP snooping VLAN assert RPC debug messages. |
| **warn** | Display IGMP snooping warning messages. |

**Note** Though visible in the command-line help strings, the **rpc l3mm** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform ip igmp snooping** command is the same as the **no debug platform ip igmp snooping** command.

## Related Commands

| Command | Description |
|---|---|
| **debug ip igmp snooping** | Displays information about platform-independent IGMP snooping activity. |
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform led

Use the **debug platform led** privileged EXEC command to enable debugging of light-emitting diode (LED) actions. Use the **no** form of this command to disable debugging.

**debug platform led** {**generic** | **signal**}

**no debug platform led** {**generic** | **signal**}

## Syntax Description

| | |
|---|---|
| **generic** | Display LED generic action debug messages. |
| **signal** | Display LED signal bit map debug messages. |

**Note** Though visible in the command-line help strings, the **stack** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform led** command is the same as the **no debug platform led** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform matm

Use the **debug platform matm** privileged EXEC command to enable debugging of platform-dependent MAC address management. Use the **no** form of this command to disable debugging.

**debug platform matm** {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

**no debug platform matm** {**aging** | **all** | **ec-aging** | **errors** | **learning** | **rpc** | **secure-address** | **warnings**}

## Syntax Description

| | |
|---|---|
| **aging** | Display MAC address aging debug messages. |
| **all** | Display all platform MAC address management event debug messages. |
| **ec-aging** | Display EtherChannel address aging-related debug messages. |
| **errors** | Display MAC address management error messages. |
| **learning** | Display MAC address management address-learning debug messages. |
| **rpc** | Display MAC address management remote procedure call (RPC) related debug messages. |
| **secure-address** | Display MAC address management secure address learning debug messages. |
| **warning** | Display MAC address management warning messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform matm** command is the same as the **no debug platform matm** command.

## Related Commands

| Command | Description |
|---|---|
| **debug matm** | Displays information about platform-independent MAC address management. |
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform messaging application

Use the **debug platform messaging application** privileged EXEC command to enable debugging of application messaging activity. Use the **no** form of this command to disable debugging.

**debug platform messaging application** {**all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr**}

**no debug platform messaging application** {**all** | **badpak** | **cleanup** | **events** | **memerr** | **messages** | **usererr**}

## Syntax Description

| | |
|---|---|
| **all** | Display all application-messaging debug messages. |
| **badpak** | Display bad-packet debug messages. |
| **cleanup** | Display clean-up debug messages. |
| **events** | Display event debug messages. |
| **memerr** | Display memory-error debug messages. |
| **messages** | Display application-messaging debug messages. |
| **usererr** | Display user-error debug messages. |

**Note** Though visible in the command-line help strings, the **stackchg** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform messaging application** command is the same as the **no debug platform messaging application** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform phy

Use the **debug platform phy** privileged EXEC command to enable debugging of PHY driver information. Use the **no** form of this command to disable debugging.

**debug platform phy** {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write**}

**no debug platform phy** {**automdix** | **cablediag** | **dual-purpose** | **flcd** {**configure** | **ipc** | **iter** | **trace**} | **flowcontrol** | **forced** | **init-seq** | **link-status** | **read** | **sfp** | **show-controller** | **speed** | **write**}

## Syntax Description

| | |
|---|---|
| **automdix** | Display PHY automatic medium-dependent interface crossover (Auto-MDIX) debug messages. |
| **cablediag** | Display PHY cable-diagnostic debug messages. |
| **dual-purpose** | Display dual-purpose PHY events. |
| **flcd** {**configure** \| **ipc** \| **iter** \| **trace**} | Display PHY FLCD debug messages. The keywords have these meanings:<br>• **configure**—Display PHY configure debug messages.<br>• **ipc**—Display Interprocess Communication Protocol (IPC) debug messages.<br>• **iter**—Display iter debug messages.<br>• **trace**—Display trace debug messages. |
| **flowcontrol** | Display PHY flowcontrol debug messages. |
| **forced** | Display PHY forced-mode debug messages. |
| **init-seq** | Display PHY initialization-sequence debug messages. |
| **link-status** | Display PHY link-status debug messages. |
| **read** | Display PHY-read debug messages. |
| **sfp** | Display PHY small form-factor pluggable (SFP) modules debug messages. |
| **show-controller** | Display PHY show-controller debug messages. |
| **speed** | Display PHY speed-change debug messages. |
| **write** | Display PHY-write debug messages. |

**Note** Although visible in the command-line help, the **xenpak** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

The **undebug platform phy** command is the same as the **no debug platform phy** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform pm

Use the **debug platform pm** privileged EXEC command to enable debugging of the platform-dependent port manager software module. Use the **no** form of this command to disable debugging.

**debug platform pm** {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput** | **sync** | **vlans**}

**no debug platform pm** {**all** | **counters** | **errdisable** | **etherchnl** | **exceptions** | **hpm-events** | **idb-events** | **if-numbers** | **ios-events** | **link-status** | **platform** | **pm-events** | **pm-vectors** [**detail**] | **rpc** [**general** | **oper-info** | **state** | **vectors** | **vp-events**] | **soutput** | **sync** | **vlans**}

## Syntax Description

| | |
|---|---|
| **all** | Display all port-manager debug messages. |
| **counters** | Display counters for remote procedure call (RPC) debug messages. |
| **errdisable** | Display error-disabled related-events debug messages. |
| **etherchnl** | Display EtherChannel related-events debug messages. |
| **exceptions** | Display system exception debug messages. |
| **hpm-events** | Display platform port-manager event debug messages. |
| **idb-events** | Display interface descriptor block (IDB) related-events debug messages. |
| **if-numbers** | Display interface-number translation-event debug messages. |
| **ios-events** | Display IOS event debug messages. |
| **link-status** | Display interface link-detection event debug messages. |
| **platform** | Display port-manager function-event debug messages. |
| **pm-events** | Display port manager event debug messages. |
| **pm-vectors** [**detail**] | Display port-manager vector-related-event debug messages. The keyword has this meaning:<br>• **detail**—Display vector-function details. |
| **rpc** [**general** \| **oper-info** \| **state** \| **vectors** \| **vp-events**] | Display RPC related-event debug messages. The keywords have these meanings:<br>• **general**—(Optional) Display RPC general events.<br>• **oper-info**—(Optional) Display operational- and informational-related RPC messages.<br>• **state**—(Optional) Display administrative- and operational-related RPC messages.<br>• **vectors**—(Optional) Display vector-related RPC messages.<br>• **vp-events**—(Optional) Display virtual ports related-events RP messages. |
| **soutput** | Display IDB output vector event debug messages. |
| **sync** | Display operational synchronization and VLAN line-state event debug messages. |
| **vlans** | Display VLAN creation and deletion event debug messages. |

**Note** Though visible in the command-line help strings, the **stack-manager** keyword is not supported.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

The **undebug platform pm** command is the same as the **no debug platform pm** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform policer cpu uni-eni

Use the **debug platform policer cpu uni-eni** privileged EXEC command to enable debugging of the control-plane policer for user network interfaces (UNIs) and enhanced network interfaces (ENIs). This command displays information messages when any changes are made to CPU protection. Use the **no** form of this command to disable debugging.

**debug platform policer cpu uni-eni**

**no debug platform policer cpu uni-eni**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |
| 12.2(44)SE | The command was changed from **debug platform policer cpu uni** to **debug platform policer cpu uni-eni.** |

## Usage Guidelines

The **undebug platform policer cpu uni-eni** command is the same as the **no debug platform policer cpu uni-eni** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show platform policer cpu** | Displays control plane policer statistics per feature or the indexes and the corresponding feature for the specified port. |

# debug platform port-asic

Use the **debug platform port-asic** privileged EXEC command to enable debugging of the port application-specific integrated circuit (ASIC) driver. Use the **no** form of this command to disable debugging.

**debug platform port-asic** {**interrupt** | **periodic** | **read** | **write**}

**no debug platform port-asic** {**interrupt** | **periodic** | **read** | **write**}

## Syntax Description

| | |
|---|---|
| **interrupt** | Display port-ASIC interrupt-related function debug messages. |
| **periodic** | Display port-ASIC periodic-function-call debug messages. |
| **read** | Display port-ASIC read debug messages. |
| **write** | Display port-ASIC write debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform port-asic** command is the same as the **no debug platform port-asic** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform port-security

Use the **debug platform port-security** privileged EXEC command to enable debugging of platform-dependent port-security information. Use the **no** form of this command to disable debugging.

**debug platform port-security** {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

**no debug platform port-security** {**add** | **aging** | **all** | **delete** | **errors** | **rpc** | **warnings**}

## Syntax Description

| | |
|---|---|
| **add** | Display secure address addition debug messages. |
| **aging** | Display secure address aging debug messages. |
| **all** | Display all port-security debug messages. |
| **delete** | Display secure address deletion debug messages. |
| **errors** | Display port-security error debug messages. |
| **rpc** | Display remote procedure call (RPC) debug messages. |
| **warnings** | Display warning debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform port-security** command is the same as the **no debug platform port-security** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform qos-acl-tcam

Use the **debug platform qos-acl-tcam** privileged EXEC command to enable debugging of the quality of service (QoS) and access control list (ACL) ternary content addressable memory (TCAM) manager software. Use the **no** form of this command to disable debugging.

**debug platform qos-acl-tcam** {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

**no debug platform qos-acl-tcam** {**all** | **ctcam** | **errors** | **labels** | **mask** | **rpc** | **tcam**}

## Syntax Description

| | |
|---|---|
| **all** | Display all QoS and ACL TCAM (QATM) manager debug messages. |
| **ctcam** | Display Cisco TCAM (CTCAM) related-events debug messages. |
| **errors** | Display QATM error-related-events debug messages. |
| **labels** | Display QATM label-related-events debug messages. |
| **mask** | Display QATM mask-related-events debug messages. |
| **rpc** | Display QATM remote procedure call (RPC) related-events debug messages. |
| **tcam** | Display QATM TCAM-related events debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform qos-acl-tcam** command is the same as the **no debug platform qos-acl-tcam** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform remote-commands

Use the **debug platform remote-commands** privileged EXEC command to enable debugging of remote commands. Use the **no** form of this command to disable debugging.

**debug platform remote-commands**

**no debug platform remote-commands**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform remote-commands** command is the same as the **no debug platform remote-commands** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform resource-manager

Use the **debug platform resource-manager** privileged EXEC command to enable debugging of the resource manager software. Use the **no** form of this command to disable debugging.

**debug platform resource-manager** {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

**no debug platform resource-manager** {**all** | **dm** | **erd** | **errors** | **madmed** | **sd** | **stats** | **vld**}

## Syntax Description

| | |
|---|---|
| **all** | Display all resource manager debug messages. |
| **dm** | Display destination-map debug messages. |
| **erd** | Display equal-cost-route descriptor-table debug messages. |
| **errors** | Display error debug messages. |
| **madmed** | Display the MAC address descriptor table and multi-expansion descriptor table debug messages. |
| **sd** | Display the station descriptor table debug messages. |
| **stats** | Display statistics debug messages. |
| **vld** | Display the VLAN-list descriptor debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform resource-manager** command is the same as the **no debug platform resource-manager** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform snmp

Use the **debug platform snmp** privileged EXEC command to enable debugging of the platform-dependent Simple Network Management Protocol (SNMP) software. Use the **no** form of this command to disable debugging.

**debug platform snmp**

**no debug platform snmp**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform snmp** command is the same as the **no debug platform snmp** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform span

Use the **debug platform span** privileged EXEC command to enable debugging of the platform-dependent Switched Port Analyzer (SPAN) software. Use the **no** form of this command to disable debugging.

**debug platform span**

**no debug platform span**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform span** command is the same as the **no debug platform span** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform supervisor-asic

Use the **debug platform supervisor-asic** privileged EXEC command to enable debugging of the supervisor application-specific integrated circuit (ASIC). Use the **no** form of this command to disable debugging.

**debug platform supervisor-asic** {**all** | **errors** | **receive** | **send**}

**no debug platform supervisor-asic** {**all** | **errors** | **receive** | **send**}

## Syntax Description

| | |
|---|---|
| **all** | Display all supervisor-ASIC event debug messages. |
| **errors** | Display the supervisor-ASIC error debug messages. |
| **jumbo** | Display the supervisor-ASIC jumbo debug messages. |
| **receive** | Display the supervisor-ASIC receive debug messages. |
| **send** | Display the supervisor-ASIC send debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform supervisor-asic** command is the same as the **no debug platform supervisor-asic** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform sw-bridge

Use the **debug platform sw-bridge** privileged EXEC command to enable debugging of the software bridging function. Use the **no** form of this command to disable debugging.

**debug platform sw-bridge** {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

**no debug platform sw-bridge** {**broadcast** | **control** | **multicast** | **packet** | **unicast**}

## Syntax Description

| | |
|---|---|
| **broadcast** | Display broadcast-data debug messages. |
| **control** | Display protocol-packet debug messages. |
| **multicast** | Display multicast-data debug messages. |
| **packet** | Display sent and received data debug messages. |
| **unicast** | Display unicast-data debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform sw-bridge** command is the same as the **no debug platform sw-bridge** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform tcam

Use the **debug platform tcam** privileged EXEC command to enable debugging of ternary content addressable memory (TCAM) access and lookups. Use the **no** form of this command to disable debugging.

**debug platform tcam** {**log** | **read** | **search** | **write**}

**debug platform tcam log l2** {**acl** {**input** | **output**} | **local** | **qos**}

**debug platform tcam read** {**reg** | **ssram** | **tcam**}

**debug platform tcam search**

**debug platform tcam write** {**forw-ram** | **reg** | **tcam**}

**no debug platform tcam** {**log** | **read** | **search** | **write**}

**no debug platform tcam log l2** {**acl** {**input** | **output**} | **local** | **qos**}

**no debug platform tcam read** {**reg** | **ssram** | **tcam**}

**no debug platform tcam search**

**no debug platform tcam write** {**forw-ram** | **reg** | **tcam**}

## Syntax Description

| | |
|---|---|
| **log l2** {**acl** {**input** \| **output**} \| **local** \| **qos**} | Display Layer 2 field-based CAM look-up type debug messages. The keywords have these meanings:<br>• **acl** {**input** \| **output**}—Display input or output ACL look-up debug messages.<br>• **local**—Display local forwarding look-up debug messages.<br>• **qos**—Display classification and quality of service (QoS) look-up debug messages. |
| **read** {**reg** \| **ssram** \| **tcam**} | Display TCAM-read debug messages. The keywords have these meanings:<br>• **reg**—Display TCAM-register read debug messages.<br>• **ssram**—Display synchronous static RAM (SSRAM)-read debug messages.<br>• **tcam**—Display TCAM-read debug messages. |
| **search** | Display supervisor-initiated TCAM-search results debug messages. |
| **write** {**forw-ram** \| **reg** \| **tcam**} | Display TCAM-write debug messages. The keywords have these meanings:<br>**forw-ram**—Display forwarding-RAM write debug messages.<br>**reg**—Display TCAM-register write debug messages.<br>**tcam**—Display TCAM-write debug messages. |

**Note** Though visible in the command-line help strings, the **log l3 acl**, **l3 ipv6** {**acl** {**input** | **output**} | **local** | **qos** | s**econdary**}, the **l3 local**, and the **l3 secondary** keywords are not supported.

**Defaults**

Debugging is disabled.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

The **undebug platform tcam** command is the same as the **no debug platform tcam** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform udld

Use the **debug platform udld** privileged EXEC command to enable debugging of the platform-dependent UniDirectional Link Detection (UDLD) software. Use the **no** form of this command to disable debugging.

**debug platform udld** [**all** | **error** | **rpc** {**events** | **messages**}]

**no debug platform udld** [**all** | **error** | **rpc** {**events** | **messages**}]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all UDLD debug messages. |
| **error** | (Optional) Display error condition debug messages. |
| **rpc** {**events** \| **messages**} | (Optional) Display UDLD remote procedure call (RPC) debug messages. The keywords have these meanings:<br>• **events**—Display UDLD RPC events.<br>• **messages**—Display UDLD RPC messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform udld** command is the same as the **no debug platform udld** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug platform vlan

Use the **debug platform vlan** privileged EXEC command to enable debugging of the VLAN manager software. Use the **no** form of this command to disable debugging.

**debug platform vlan** {**errors** | **mvid** | **rpc**}

**no debug platform vlan** {**errors** | **mvid** | **rpc**}

## Syntax Description

| | |
|---|---|
| **errors** | Display VLAN error debug messages. |
| **mvid** | Display mapped VLAN ID allocations and free debug messages. |
| **rpc** | Display remote procedure call (RPC) debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug platform vlan** command is the same as the **no debug platform vlan** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug pm

Use the **debug pm** privileged EXEC command to enable debugging of port manager (PM) activity. The port manager is a state machine that controls all the logical and physical interfaces. All features, such as VLANs, UniDirectional Link Detection (UDLD), and so forth, work with the port manager to provide switch functions. Use the **no** form of this command to disable debugging.

**debug pm** {**all** | **assert** | **card** | **cookies** | **etherchnl** | **hatable** | **messages** | **port** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

**no debug pm** {**all** | **assert** | **card** | **cookies** | **etherchnl** | **hatable** | **messages** | **port** | **registry** | **sm** | **span** | **split** | **vlan** | **vp**}

## Syntax Description

| | |
|---|---|
| **all** | Display all PM debug messages. |
| **assert** | Display assert debug messages. |
| **card** | Display line-card related-events debug messages. |
| **cookies** | Display internal PM cookie validation debug messages. |
| **etherchnl** | Display EtherChannel related-events debug messages. |
| **hatable** | Display Host Access Table events debug messages. |
| **messages** | Display PM debug messages. |
| **port** | Display port related-events debug messages. |
| **registry** | Display PM registry invocation debug messages. |
| **sm** | Display state-machine related-events debug messages. |
| **span** | Display spanning-tree related-events debug messages. |
| **split** | Display split-processor debug messages. |
| **vlan** | Display VLAN related-events debug messages. |
| **vp** | Display virtual port related-events debug messages. |

**Note** Though visible in the command-line help strings, the **scp** and **pvlan** keywords are not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug pm** command is the same as the **no debug pm** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug port-security

Use the **debug port-security** privileged EXEC command to enable debugging of the allocation and states of the port security subsystem. Use the **no** form of this command to disable debugging.

**debug port-security**

**no debug port-security**

## Syntax Description

This command has no arguments or keywords.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug port-security** command is the same as the **no debug port-security** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show port-security** | Displays port-security settings for an interface or for the switch. |

# debug qos-manager

Use the **debug qos-manager** privileged EXEC command to enable debugging of the quality of service (QoS) manager software. Use the **no** form of this command to disable debugging.

**debug qos-manager** {**all** | **event** | **verbose**}

**no debug qos-manager** {**all** | **event** | **verbose**}

## Syntax Description

| | |
|---|---|
| **all** | Display all QoS-manager debug messages. |
| **event** | Display QoS-manager related-event debug messages. |
| **verbose** | Display QoS-manager detailed debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug qos-manager** command is the same as the **no debug qos-manager** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

# debug spanning-tree

Use the **debug spanning-tree** privileged EXEC command to enable debugging of spanning-tree activities. Use the **no** form of this command to disable debugging.

**debug spanning-tree** {**all** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization**}

**no debug spanning-tree** {**all** | **bpdu** | **bpdu-opt** | **config** | **etherchannel** | **events** | **exceptions** | **general** | **mstp** | **pvst+** | **root** | **snmp** | **switch** | **synchronization**}

## Syntax Description

| | |
|---|---|
| **all** | Display all spanning-tree debug messages. |
| **bpdu** | Display spanning-tree bridge protocol data unit (BPDU) debug messages. See the **debug spanning-tree bpdu** command. |
| **bpdu-opt** | Display optimized BPDU handling debug messages. See the **debug spanning-tree bpdu-opt** command |
| **config** | Display spanning-tree configuration change debug messages. |
| **etherchannel** | Display EtherChannel-support debug messages. |
| **events** | Display spanning-tree topology event debug messages. |
| **exceptions** | Display spanning-tree exception debug messages. |
| **general** | Display general spanning-tree activity debug messages. |
| **mstp** | Debug Multiple Spanning Tree Protocol events. See the **debug spanning-tree mstp** command |
| **pvst+** | Display per-VLAN spanning-tree plus (PVST+) event debug messages. |
| **root** | Display spanning-tree root-event debug messages. |
| **snmp** | Display spanning-tree Simple Network Management Protocol (SNMP) handling debug messages. |
| **switch** | Display switch shim command debug messages. This shim is the software module that is the interface between the generic Spanning Tree Protocol (STP) code and the platform-specific code of various switch platforms. See the **debug spanning-tree switch** command |
| **synchronization** | Display the spanning-tree synchronization event debug messages. |

**Note** Though visible in the command-line help strings, the **backbonefast**, **csuf/csrt**, and **uplinkfast** keywords are not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

The **undebug spanning-tree command is the** same as the **no debug spanning-tree** command.

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show spanning-tree** | Displays spanning-tree state information. |

# debug spanning-tree bpdu

Use the **debug spanning-tree bpdu** privileged EXEC command to enable debugging of sent and received spanning-tree bridge protocol data units (BPDUs). Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu** [**receive** | **transmit**]

**no debug spanning-tree bpdu** [**receive** | **transmit**]

## Syntax Description

| | |
|---|---|
| **receive** | (Optional) Display the nonoptimized path for received BPDU debug messages. |
| **transmit** | (Optional) Display the nonoptimized path for sent BPDU debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug spanning-tree bpdu** command is the same as the **no debug spanning-tree bpdu** command**.**

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show spanning-tree** | Displays spanning-tree state information. |

# debug spanning-tree bpdu-opt

Use the **debug spanning-tree bpdu-opt** privileged EXEC command to enable debugging of optimized spanning-tree bridge protocol data units (BPDUs) handling. Use the **no** form of this command to disable debugging.

**debug spanning-tree bpdu-opt** [**detail | packet**]

**no debug spanning-tree bpdu-opt** [**detail | packet**]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Display detailed optimized BPDU-handling debug messages. |
| **packet** | (Optional) Display packet-level optimized BPDU-handling debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug spanning-tree bpdu-opt** command is the same as the **no debug spanning-tree bpdu-opt** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show spanning-tree** | Displays spanning-tree state information. |

# debug spanning-tree mstp

Use the **debug spanning-tree mstp** privileged EXEC command to enable debugging of the Multiple Spanning Tree Protocol (MSTP) software. Use the **no** form of this command to disable debugging.

**debug spanning-tree mstp** {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

**no debug spanning-tree mstp** {**all** | **boundary** | **bpdu-rx** | **bpdu-tx** | **errors** | **flush** | **init** | **migration** | **pm** | **proposals** | **region** | **roles** | **sanity_check** | **sync** | **tc** | **timers**}

## Syntax Description

| | |
|---|---|
| **all** | Enable all the debugging messages. |
| **boundary** | Debug flag changes at these boundaries:<br>• An multiple spanning-tree (MST) region and a single spanning-tree region running Rapid Spanning Tree Protocol (RSTP)<br>• An MST region and a single spanning-tree region running IEEE 802.1D<br>• An MST region and another MST region with a different configuration |
| **bpdu-rx** | Debug the received MST bridge protocol data units (BPDUs). |
| **bpdu-tx** | Debug the sent MST BPDUs. |
| **errors** | Debug MSTP errors. |
| **flush** | Debug the port flushing mechanism. |
| **init** | Debug the initialization of the MSTP data structures. |
| **migration** | Debug the protocol migration state machine. |
| **pm** | Debug MSTP port manager events. |
| **proposals** | Debug handshake messages between the designated switch and the root switch. |
| **region** | Debug the region synchronization between the switch processor (SP) and the route processor (RP). |
| **roles** | Debug MSTP roles. |
| **sanity_check** | Debug the received BPDU sanity check messages. |
| **sync** | Debug the port synchronization events. |
| **tc** | Debug topology change notification events. |
| **timers** | Debug the MSTP timers for start, stop, and expire events. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug spanning-tree mstp** command is the same as the **no debug spanning-tree mstp** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show spanning-tree** | Displays spanning-tree state information. |

# debug spanning-tree switch

Use the **debug spanning-tree switch** privileged EXEC command to enable debugging of the software interface between the Spanning Tree Protocol (STP) software module and the port manager software module. Use the **no** form of this command to disable debugging.

**debug spanning-tree switch** {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

**no debug spanning-tree switch** {**all** | **errors** | **flush** | **general** | **helper** | **pm** | **rx** {**decode** | **errors** | **interrupt** | **process**} | **state** | **tx** [**decode**]}

## Syntax Description

| | |
|---|---|
| **all** | Display all spanning-tree switch debug messages. |
| **errors** | Display debug messages for the interface between the spanning-tree software module and the port manager software module. |
| **flush** | Display debug messages for the shim flush operation. |
| **general** | Display general event debug messages. |
| **helper** | Display spanning-tree helper-task debug messages. Helper tasks handle bulk spanning-tree updates. |
| **pm** | Display port-manager event debug messages. |
| **rx** | Display received bridge protocol data unit (BPDU) handling debug messages. The keywords have these meanings:<br>• **decode**—Display decoded received packets.<br>• **errors**—Display receive error debug messages.<br>• **interrupt**—Display interrupt service request (ISR) debug messages.<br>• **process**—Display process receive BPDU debug messages. |
| **state** | Display spanning-tree port state change debug messages; |
| **tx** [**decode**] | Display sent BPDU handling debug messages. The keyword has this meaning:<br>• **decode**—(Optional) Display decoded sent packets. |

**Note** Though visible in the command-line help strings, the **uplinkfast** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug spanning-tree switch** command is the same as the **no debug spanning-tree switch** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show spanning-tree** | Displays spanning-tree state information. |

# debug sw-vlan

Use the **debug sw-vlan** privileged EXEC command to enable debugging of VLAN manager activities. Use the **no** form of this command to disable debugging.

**debug sw-vlan** {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **notification** | **packets** | **registries**}

**no debug sw-vlan** {**badpmcookies** | **cfg-vlan** {**bootup** | **cli**} | **events** | **ifs** | **management** | **notification** | **packets** | **registries**}

## Syntax Description

| | |
|---|---|
| **badpmcookies** | Display debug messages for VLAN manager incidents of bad port manager cookies. |
| **cfg-vlan** {**bootup** \| **cli**} | Display config-vlan debug messages. The keywords have these meanings:<br>• **bootup**—Display messages when the switch is booting up.<br>• **cli**—Display messages when the command-line interface (CLI) is in config-vlan mode. |
| **events** | Display debug messages for VLAN manager events. |
| **ifs** | See the **debug sw-vlan ifs** command. |
| **management** | Display debug messages for VLAN manager management of internal VLANs. |
| **notification** | See the **debug sw-vlan notification** command. |
| **packets** | Display debug messages for packet handling and encapsulation processes. |
| **registries** | Display debug messages for VLAN manager registries. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug sw-vlan** command is the same as the **no debug sw-vlan** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show vlan** | Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain. |

# debug sw-vlan ifs

Use the **debug sw-vlan ifs** privileged EXEC command to enable debugging of the VLAN manager IOS file system (IFS) error tests. Use the **no** form of this command to disable debugging.

**debug sw-vlan ifs** {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

**no debug sw-vlan ifs** {**open** {**read** | **write**} | **read** {**1** | **2** | **3** | **4**} | **write**}

## Syntax Description

| | |
|---|---|
| **open** {**read** \| **write**} | Display VLAN manager IFS file-open operation debug messages. The keywords have these meanings:<br>• **read**—Display VLAN manager IFS file-read operation debug messages.<br>• **write**—Display VLAN manager IFS file-write operation debug messages. |
| **read** {**1** \| **2** \| **3** \| **4**} | Display file-read operation debug messages for the specified error test (1, 2, 3, or 4). |
| **write** | Display file-write operation debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug sw-vlan ifs** command is the same as the **no debug sw-vlan ifs** command.

When selecting the file read operation, Operation **1** reads the file header, which contains the header verification word and the file version number. Operation **2** reads the main body of the file, which contains most of the domain and VLAN information. Operation **3** reads type length version (TLV) descriptor structures. Operation **4** reads TLV data.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show vlan** | Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain. |

# debug sw-vlan notification

Use the **debug sw-vlan notification** privileged EXEC command to enable debugging of the activation and deactivation of VLAN IDs. Use the **no** form of this command to disable debugging.

**debug sw-vlan notification** {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **statechange**}

**no debug sw-vlan notification** {**accfwdchange** | **allowedvlancfgchange** | **fwdchange** | **linkchange** | **modechange** | **statechange**}

## Syntax Description

| | |
|---|---|
| **accfwdchange** | Display debug messages for VLAN manager notification of aggregated access interface spanning-tree forward changes. |
| **allowedvlancfgchange** | Display debug messages for VLAN manager notification of changes to the allowed VLAN configuration. |
| **fwdchange** | Display debug messages for VLAN manager notification of spanning-tree forwarding changes. |
| **linkchange** | Display debug messages for VLAN manager notification of interface link-state changes. |
| **modechange** | Display debug messages for VLAN manager notification of interface mode changes. |
| **statechange** | Display debug messages for VLAN manager notification of interface state changes. |

**Note** Though visible in the command-line help strings, the **pruningcfgchange** keyword is not supported.

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug sw-vlan notification** command is the same as the **no debug sw-vlan notification** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show vlan** | Displays the parameters for all configured VLANs or one VLAN (if the VLAN name or ID is specified) in the administrative domain. |

# debug udld

Use the **debug udld** privileged EXEC command to enable debugging of the UniDirectional Link Detection (UDLD) feature. Use the **no** form of this command to disable UDLD debugging.

**debug udld** {**events** | **packets** | **registries**}

**no debug udld** {**events** | **packets** | **registries**}

## Syntax Description

| | |
|---|---|
| **events** | Display debug messages for UDLD process events as they occur. |
| **packets** | Display debug messages for the UDLD process as it receives packets from the packet queue and tries to send them at the request of the UDLD protocol code. |
| **registries** | Display debug messages for the UDLD process as it processes registry calls from the UDLD process-dependent module and other feature modules. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug udld** command is the same as the **no debug udld** command.

For **debug udld events**, these debugging messages appear:

- General UDLD program logic flow
- State machine state changes
- Program actions for the set and clear ErrDisable state
- Neighbor cache additions and deletions
- Processing of configuration commands
- Processing of link-up and link-down indications

For **debug udld packets**, these debugging messages appear:

- General packet processing program flow on receipt of an incoming packet
- Indications of the contents of the various pieces of packets received (such as type length versions [TLVs]) as they are examined by the packet reception code
- Packet transmission attempts and the outcome

For **debug udld registries**, these categories of debugging messages appear:

- Sub-block creation
- Fiber-port status changes
- State change indications from the port manager software
- MAC address registry calls

**Related Commands**

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |
| **show udld** | Displays UDLD administrative and operational status for all ports or the specified port. |

# debug vqpc

Use the **debug vqpc** privileged EXEC command to enable debugging of the VLAN Query Protocol (VQP) client. Use the **no** form of this command to disable debugging.

**debug vqpc** [**all** | **cli** | **events** | **learn** | **packet**]

**no debug vqpc** [**all** | **cli** | **events** | **learn** | **packet**]

## Syntax Description

| | |
|---|---|
| **all** | (Optional) Display all VQP client debug messages. |
| **cli** | (Optional) Display the VQP client command-line interface (CLI) debug messages. |
| **events** | (Optional) Display VQP client event debug messages. |
| **learn** | (Optional) Display VQP client address learning debug messages. |
| **packet** | (Optional) Display VQP client packet information debug messages. |

## Defaults

Debugging is disabled.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

The **undebug vqpc** command is the same as the **no debug vqpc** command.

## Related Commands

| Command | Description |
|---|---|
| **show debugging** | Displays information about the types of debugging that are enabled. |

APPENDIX C

# Cisco ME 2400 Ethernet Access Switch Show Platform Commands

This appendix describes the **show platform** privileged EXEC commands that have been created or changed for use with the Cisco ME 2400 Ethernet Access switch. These commands display information helpful in diagnosing and resolving internetworking problems and should be used only under the guidance of Cisco technical support staff.

# show platform acl

Use the **show platform acl** privileged EXEC command to display platform-dependent access control list (ACL) manager information.

**show platform acl** {**interface** *interface-id* | **label** *label-number* [**detail**] | **statistics** *asic-number* | **usage** *asic-number* [**summary**] | **vlan** *vlan-id*} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **interface** *interface-id* | Display per-interface ACL manager information for the specified interface. The interface can be a physical interface or a VLAN. |
| **label** *label-number* [**detail**] | Display per-label ACL manager information. The *label-number* range is 0 to 255. The keyword has this meaning:<br>• **detail**—(Optional) Display detailed ACL manager label information. |
| **statistics** *asic-number* | Display per-ASIC ACL statistics. The *asic-numbe*r is the port ASIC number, always 0. |
| **usage** *asic-number* [**summary**] | Display per-ASIC ACL usage. The *asic-numbe*r is the port ASIC number, always 0. The keyword has this meaning:<br>• **summary**—(Optional) Display brief usage information. |
| **vlan** *vlan-id* | Display per-VLAN ACL manager information. The *vlan-id* range is from 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform configuration

Use the **show platform configuration** privileged EXEC command to display platform-dependent configuration-manager related information.

**show platform configuration** {**config-output** | **default** | **running** | **startup**} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **config-output** | Display the output of the last auto-configuration application. |
| **default** | Display whether or not the system is running the default configuration. |
| **running** | Display a snapshot of the backed-up running configuration on the local switch. |
| **startup** | Display a snapshot of the backed-up startup configuration on the local switch. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform etherchannel

Use the **show platform etherchannel** privileged EXEC command to display platform-dependent EtherChannel information.

**show platform etherchannel** {**flags** | **time-stamps**} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **flags** | Display EtherChannel port flags. |
| **time-stamps** | Display EtherChannel time stamps. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform forward

Use the **show platform forward** privileged EXEC command for an interface to specify how the hardware would forward a frame that matches the specified parameters.

**show platform forward** *interface-id* [**vlan** *vlan-id*] *src-mac dst-mac* [*l3protocol-id*] [**sap** | **snap**] [**cos** *cos*] [**ip** *src-ip dst-ip* [**frag** *field*] [**dscp** *dscp*] {*l4protocol-id* | **icmp** *icmp-type icmp-code* | **igmp** *igmp-version igmp-type* | **tcp** *src-port dst-port flags* | **udp** *src-port dst-port*} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| *interface-id* | The input physical interface, the port on which the packet comes in to the switch (including type and port number). |
| **vlan** *vlan-id* | (Optional) Input VLAN ID. The range is 1 to 4094. If not specified, and the input interface is not a routed port, the default is 1. |
| *src-mac* | 48-bit source MAC address. |
| *dst-mac* | 48-bit destination MAC address. |
| *l3protocol-id* | (Optional) The Layer 3 protocol used in the packet. The number is a value 0 to 65535. |
| **sap** | (Optional) Service access point (SAP) encapsulation type. |
| **snap** | (Optional) Subnetwork Access Protocol (SNAP) encapsulation type. |
| **cos** *cos* | (Optional) Class of service (CoS) value of the frame. The range is 0 to 7. |
| **ip** *src-ip dst-ip* | (Optional, but required for IP packets) Source and destination IP addresses in dotted decimal notation. |
| **frag** *field* | (Optional) The IP fragment field for a fragmented IP packet. The range is 0 to 65535. |
| **dscp** *dscp* | (Optional) Differentiated Services Code Point (DSCP) field in the IP header. The range is 0 to 63. |
| *l4protocol-id* | The numeric value of the Layer 4 protocol field in the IP header. The range is 0 to 255. For example, 47 is generic routing encapsulation (GRE), and 89 is Open Shortest Path First (OSPF). If the protocol is TCP, UDP, ICMP, or IGMP, you should use the appropriate keyword instead of a numeric value. |
| **icmp** *icmp-type icmp-code* | Internet Control Message Protocol (ICMP) parameters. The *icmp-type* and *icmp-code* ranges are 0 to 255. |
| **igmp** *igmp-version igmp-type* | Internet Group Management Protocol (IGMP) parameters. The *igmp-version* range is 1 to 15; the *igmp-type* range is 0 to 15. |
| **tcp** *src-port dst-port flags* | TCP parameters: TCP source port, destination port, and the numeric value of the TCP flags byte in the header. The *src-port* and *dst-port* ranges are 0 to 65535. The flag range is from 0 to 1024. |
| **udp** *src-port dst-port* | User Datagram Protocol (UDP) parameters. The *src-port* and *dst-port* ranges are 0 to 65535. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **ipv6** keyword is not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

## Examples

See the "Troubleshooting" chapter of the software configuration guide for this release for examples of the **show platform forward** command output displays and what they mean.

# show platform ip igmp snooping

Use the **show platform ip igmp snooping** privileged EXEC command to display platform-dependent Internet Group Management Protocol (IGMP) snooping information.

**show platform ip igmp snooping** {**all** | **control** [**di**] | **counters** | **flood** [**vlan** *vlan-id*] | **group** *ip-address* | **hardware** | **retry** [**count** | **local** [**count**] | **remote** [**count**]]} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **all** | Display all IGMP snooping platform IP multicast information. |
| **control** [**di**] | Display IGMP snooping control entries. The keyword has this meaning:<br>• **di**—(Optional) Display IGMP snooping control destination index entries. |
| **counters** | Display IGMP snooping counters. |
| **flood** [**vlan** *vlan-id*] | Display IGMP snooping flood information. The keyword has this meaning:<br>• **vlan** *vlan-id*—(Optional) Display flood information for the specified VLAN. The range is 1 to 4094. |
| **group** *ip-address* | Display the IGMP snooping multicast group information, where *ip-address* is the IP address of the group. |
| **hardware** | Display IGMP snooping information loaded into hardware. |
| **retry** [**count** \| **local** [**count**] | Display IGMP snooping retry information. The keywords have these meanings:<br>• **count**—(Optional) Display only the retry count.<br>• **local**—(Optional) Display local retry entries. |
| **remote** [**count**] | Display remote entries. The keyword has this meaning:<br>• **count**—(Optional) Display only the remote count. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform layer4op

Use the **show platform layer4op** privileged EXEC command to display platform-dependent Layer 4 operator information.

**show platform layer4op** {**acl** | **qos** [*port-asic*]} {**and-or** | **map** | **or-and** | **vcu**} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **acl** | Display access control list (ACL) Layer 4 operators information. |
| **qos** [*port-asic*] | Display quality of service (QoS) Layer 4 operators information. The keyword has this meaning:<br>• *port-asic*—(Optional) QoS port ASIC number. The value can be 0 or 1. |
| **and-or** | Display AND-OR registers information. |
| **map** | Display select map information. |
| **or-and** | Display OR-AND registers information. |
| **vcu** | Display value compare unit (VCU) register information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform mac-address-table

Use the **show platform mac-address-table** privileged EXEC command to display platform-dependent MAC address table information.

**show platform mac-address-table** [**aging-array** | **hash-table** | **mac-address** *mac-address*] [**vlan** *vlan-id*]] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **aging-array** | (Optional) Display the MAC address table aging array. |
| **hash-table** | (Optional) Display the MAC address table hash table. |
| **mac-address** *mac-address* | (Optional) Display the MAC address table MAC address information, where *mac-address* is the 48-bit hardware address. |
| **vlan** *vlan-id* | (Optional) Display information for the specified VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform messaging

Use the **show platform messaging** privileged EXEC command to display platform-dependent application and performance message information.

**show platform messaging** {**application** [**incoming** | **outgoing** | **summary**] | **hiperf** [*class-number*]} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **application** [**incoming** \| **outgoing** \| **summary**] | Display application message information. The keywords have these meanings:<br>• **incoming**—(Optional) Display only information about incoming application messaging requests.<br>• **outgoing**—(Optional) Display only information about incoming application messaging requests.<br>• **summary**—(Optional) Display summary information about all application messaging requests. |
| **hiperf** [*class-number*] | Display outgoing high-performance message information. Specify the *class-number* option to display information about high-performance messages for this class number. The range is 0 to 36. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform monitor

Use the **show platform monitor** privileged EXEC command to display platform-dependent Switched Port Analyzer (SPAN) information.

**show platform monitor** [**session** *session-number*] [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **session** *session-number* | (Optional) Display SPAN information for the specified SPAN session. The range is 1 to 66. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform mvr table

Use the **show platform mvr table** privileged EXEC command to display the platform-dependent Multicast VLAN Registration (MVR) multi-expansion descriptor (MED) group mapping table.

**show platform mvr table** [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with a technical support representative while troubleshooting a problem. Do not use this command unless a technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform pm

Use the **show platform pm** privileged EXEC command to display platform-dependent port-manager information.

**show platform pm** {**counters** | **group-masks** | **idbs** {**active-idbs** | **deleted-idbs**} | **if-numbers** | **link-status** | **platform-block** | **port-info** *interface-id* | **vlan** {**info** | **line-state**} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **counters** | Display module counters information. |
| **group-masks** | Display EtherChannel group masks information. |
| **idbs** {**active-idbs** \| **deleted-idbs**} | Display interface data block (IDB) information. The keywords have these meanings:<br>• **active-idbs**—Display active IDB information.<br>• **deleted-idbs**—Display deleted and leaked IDB information. |
| **if-numbers** | Display interface numbers information. |
| **link-status** | Display local port link status information. |
| **platform-block** | Display platform port block information. |
| **port-info** *interface-id* | Display port administrative and operation fields for the specified interface. |
| **vlan** {**info** \| **line-state**} | Display platform VLAN information. The keywords have these meanings:<br>• **info**—Display information for active VLANs.<br>• **line-state**—Display line-state information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **stack-view** keyword is not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform policer cpu

Use the **show platform policer cpu** privileged EXEC command to display CPU control-plane policer statistics per feature or the indexes and the corresponding feature for the specified port.

**show platform policer cpu** {**classification** | **interface** *interface-id*} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **classification** | Displays policer statistics per feature. |
| **interface** *interface-id* | Display the policer indexes for a specific interface. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

For CPU protection of user network interfaces (UNIs) and enhanced network interfaces (ENIs), the switch pre-allocates the 27 CPU protection policers, numbered 0 to 26. A policer of 26 means a drop policer; any traffic type shown as 26 on any port is dropped. A policer of a value of 0 to 25 means that a rate-limiting policer is assigned to the port for the control protocol. A policer value of 255 means that no policer is assigned to a control protocol. Network node interfaces (NNIs) have no policers assigned.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* are not displayed, but the lines that contain *Output* are displayed.

## Examples

This is an example of output from the **show platform policer cpu classification** command:

```
Switch# show platform policer cpu classification
================================================
SWITCH 1
================================================
Feature                        Bytes         Frames
================================================
STP                            3912792         61278
LACP                           0               0
8021X                          0               0
RSVD_STP                       0               0
PVST_PLUS                      0               0
CDP                            1012542         2552
DTP                            131264          2051
UDLD                           0               0
PAGP                           0               0
```

```
VTP                             0               0
CISCO_L2                        0               0
KEEPALIVE                       0               0
CFM                             0               0
SWITCH_MAC                      0               0
SWITCH_ROUTER_MAC               896             14
SWITCH_IGMP                     289408          4522
SWITCH_L2PT                     0               0
```

This example of the output from the **show platform policer cpu interface** command shows the default policer configuration for a UNI. Because the port is Fast Ethernet 1, the identifier for rate-limited protocols is 0; a display for Fast Ethernet port 5 would display an identifier of 4. The *Policer Index* refers to the specific protocol. The ASIC number indicates when the policer is on a different ASIC.

Because UNIs do not support STP, CDP, LLDP, LACP, and PAgP, these packets are dropped (physical policer of 26). These protocols are disabled by default on ENIs as well, but you can enable them. When enabled on ENIs, the control packets are rate-limited and a rate-limiting policers is assigned to the port for these protocols (physical policer of 22).

```
Switch# show platform policer cpu interface fastethernet 0/3
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/1
STP                                 1             26             0
LACP                                2             26             0
8021X                               3             26             0
RSVD_STP                            4             26             0
PVST_PLUS                           5             26             0
CDP                                 6             26             0
LLDP                                7             26             0
DTP                                 8             26             0
UDLD                                9             26             0
PAGP                               10             26             0
VTP                                11             26             0
CISCO_L2                           12             26             0
KEEPALIVE                          13              0             0
CFM                                14            255             0
SWITCH_MAC                         15             26             0
SWITCH_ROUTER_MAC                  16             26             0
SWITCH_IGMP                        17              0             0
SWITCH_L2PT                        18             26             0
```

This example shows the policers assigned to a ENI when control protocols are enabled on the interface. A value of 22 indicates that protocol packets are rate-limited for that protocol. When the protocol is not enabled, the defaults are the same as for a UNI.

```
Switch# show platform policer cpu interface fastethernet0/23
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Fa0/23
STP                                 1             26             0
LACP                                2             22             0
8021X                               3             26             0
RSVD_STP                            4             26             0
PVST_PLUS                           5             26             0
CDP                                 6             22             0
LLDP                                7             26             0
```

```
DTP                                8            26             0
UDLD                               9            26             0
PAGP                              10            26             0
VTP                               11            26             0
CISCO_L2                          12            22             0
KEEPALIVE                         13            22             0
CFM                               14           255             0
SWITCH_MAC                        15            26             0
SWITCH_ROUTER_MAC                 16            26             0
SWITCH_IGMP                       17            22             0
SWITCH_L2PT                       18            22             0
```

This example shows the default policers assigned to NNIs. Most protocols have no policers assigned to NNIs. A value of 255 means that no policer is assigned to the port for the protocol.

```
Switch #show platform policer cpu interface gigabitethernet 0/1
Policers assigned for CPU protection
=====================================================================
 Feature                          Policer        Physical      Asic
                                  Index          Policer       Num
=====================================================================
Gi0/1
STP                                1            255             0
LACP                               2            255             0
8021X                              3            255             0
RSVD_STP                           4            255             0
PVST_PLUS                          5            255             0
CDP                                6            255             0
LLDP                               7            255             0
DTP                                8            255             0
UDLD                               9            255             0
PAGP                              10            255             0
VTP                               11            255             0
CISCO_L2                          12            255             0
KEEPALIVE                         13            255             0
CFM                               14            255             0
SWITCH_MAC                        15            255             0
SWITCH_ROUTER_MAC                 16            255             0
SWITCH_IGMP                       17            255             0
SWITCH_L2PT                       18            255             0
```

## Related CommandsS

| Command | Description |
|---|---|
| **show policer cpu uni-eni** | Displays control-plane policer information for the switch. |

# show platform port-asic

Use the **show platform port-asic** privileged EXEC command to display platform-dependent port application-specific integrated circuit (ASIC) register information.

**show platform port-asic** {**cpu-queue-map-table** [**asic** *number* | **port** *number* [**asic** *number*]] |
**dest-map index** *number* | **etherchannel-info** [**asic** *number* | **port** *number* [**asic** *number*]] |
**exception** [**asic** *number* | **port** *number* [**asic** *number*]] | **global-status** [**asic** *number* |
**port** *number* [**asic** *number*]] | **learning** [**asic** *number* | **port** *number* [**asic** *number*]] |
**mac-info** [**asic** *number* | **port** *number* [**asic** *number*]] | **mvid** [**asic** *number*] |
**packet-info-ram** [**asic** *number* | **index** *number* [**asic** *number*]] |
**port-info** [**asic** *number* | **port** *number* [**asic** *number*]] |
**prog-parser** [**asic** *number* | **port** *number* [**asic** *number*]] |
**receive** {**buffer-queue** | **port-fifo** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]] | **span** [*vlan-id* [**asic** *number*] | [**asic** *number*]
**stats** {**drop** | **enqueue** | **miscellaneous** | **supervisor**} [**asic** *number* | **port** *number* [**asic** *number*]] |
**transmit** {**port-fifo** | **queue** | **supervisor-sram**} [**asic** *number* | **port** *number* [**asic** *number*]]
**vct** [**asic** *number* | **port** *number* [**asic** *number*]]}
[ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **cpu-queue-map-table** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the CPU queue-map table entries. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27. |
| **dest-map index** *number* | Display destination-map information for the specified index. The range is 0 to 65535. |
| **etherchannel-info** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the contents of the EtherChannel information register. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **exception** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the exception-index register information. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |

| | |
|---|---|
| **global-status** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display global and interrupt status. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **learning** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display entries in the learning cache. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **mac-info** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the contents of the MAC information register. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **mvid** [**asic** *number*] | Display the mapped VLAN ID table. The keyword has this meaning:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0. |
| **packet-info-ram** [**asic** *number* \| **index** *number* [**asic** *number*]] | Display the packet information RAM. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **index** *number*—(Optional) Display information for the specified packet RAM index number and ASIC number. The range is 0 to 63. |
| **port-info** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display port information register values. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |

| | |
|---|---|
| **prog-parser** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the programmable parser tables. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **receive** {**buffer-queue** \| **port-fifo** \| **supervisor-sram**} [**asic** *number* \| **port** *number* [**asic** *number*]] | Display receive information. The keywords have these meanings:<br>• **buffer-queue**—Display the buffer queue information.<br>• **port-fifo**—Display the port-FIFO information.<br>• **supervisor-sram**—Display the supervisor static RAM (SRAM) information.<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **span** [*vlan-id* \| **asic** *number*] | Display the Switched Port Analyzer (SPAN)-related information. The keywords have these meanings:<br>• *vlan-id*—(Optional) Display information for the specified VLAN. The range is 0 to 1023.<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0. |
| **stats** {**drop** \| **enqueue** \| **miscellaneous** \| **supervisor**} [**asic** *number* \| **port** *number* [**asic** *number*]] | Display raw statistics for the port ASIC. The keywords have these meanings:<br>• **drop**—Display drop statistics.<br>• **enqueue**—Display enqueue statistics.<br>• **miscellaneous**—Display miscellaneous statistics.<br>• **supervisor**—Display supervisor statistics.<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The number is always 0.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |

| | |
|---|---|
| **transmit** {**port-fifo** \| **queue** \| **supervisor-sram**} [**asic** *number* \| **port** *number* [**asic** *number*]] | Display transmit information. The keywords have these meanings:<br>• **port-fifo**—Display the contents of the port-FIFO information register.<br>• **queue**—Display the contents of the queue information register.<br>• **supervisor-sram**—Display supervisor SRAM information.<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **vct** [**asic** *number* \| **port** *number* [**asic** *number*]] | Display the VLAN compression table entries for the specified ASIC or for the specified port and ASIC. The keywords have these meanings:<br>• **asic** *number*—(Optional) Display information for the specified ASIC. The range is 0 to 1.<br>• **port** *number*—(Optional) Display information for the specified port and ASIC number. The range is 0 to 27, where 0 is the supervisor and 1 to 25 are the ports. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **stack** {**control** \| **dest-map** \| **learning** \| **messages** \| **mvid** \| **prog-parser** \| **span** \| **stats** [**asic** *number* \| **port** *number* [**asic** *number*]] keywords are not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **\| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform port-security

Use the **show platform port-security** privileged EXEC command to display platform-dependent port-security information.

**show platform port-security** [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform qos

Use the **show platform qos** privileged EXEC command to display platform-dependent quality of service (QoS) information.

**show platform qos debug** [**aggregate-policer** *aggregate-policer-name* | **global-config** | **input-queue** | [**interface** [*interface-id*] [**buffers** | **policers** | **queuing**] ] | **label-table** [**dynamic-label** {**dscp** *value* **cos** *value* | **label-number** *value* | **policy-map** *policy-map-name* **class-map** *class-map-name*} [**asic** *number*] | **policer** {**parameter-table** | **qos-table**| **selection-table**} [**asic** *number*] | **policy-map** *policy-map-name* [**asic** *number*] | **port-class** [**asic** *number*] | **port-config** ***port-number*** [**asic** *number*] | **port-info** *port-numbe***r** [**asic** *number*] | **table-map** | **vlan** *vlan-id*] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform qos statistics** [**interface** [*interface-id*] ] [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **debug** | Display QoS debug messages for the switch or for the specified keyword. |
| **aggregate-policer** *aggregate-policer-name* | (Optional) Display QoS aggregate policer information for the specified aggregate policer. |
| **global-config** | (Optional) Display QoS global configuration information. |
| **input-queue** | (Optional) Display QoS input queue information. |
| **interface** [*interface-id*] [**buffers** \| **policers** \| **queuing**] | (Optional) Display QoS information for all interfaces or the specified interface. The keywords have these meanings:<br>• **buffers**—(Optional) Display information about QoS buffers.<br>• **policers**—(Optional) Display information about QoS policers.<br>• **queuing**—(Optional) Display information about QoS output queues. |
| **label-table** [**dynamic-label** {**dscp** *value* **cos** *value* \| **label-number** *value* \| **policy-map** *policy-map-name* **class-map** *class-map-name*} [**asic** *number*] | (Optional) Display Qos label table information. The keywords have these meanings:<br>• **dynamic-label**—(Optional) Display dynamic label information.<br>• **dscp** *value* **cos** *value*—Display information based on Differentiated Services Code Point (DSCP) value (0 to 63) and class of service (CoS) value (0 to 7).<br>• **label-number** *value*—Display information based on the dynamic label number. The range is from 158 to 255.<br>• **policy-map** *policy-map-name* **class-map** *class-map-name*—Display information for the specified policy map and class map.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |

| | |
|---|---|
| **policer** {**parameter-table** \| **qos-table**\| **selection-table**} [**asic** *number*] | (Optional) Display QoS policer information. The keywords have these meanings:<br>• **parameter-table**—Display the policer parameter table.<br>• **qos-table**—Display the policer QoS table.<br>• **selection-table**—Display the port allocation table.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **policy-map** *policy-map-name* [**asic** *number*] | (Optional) Display QoS information for the specified policy map.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **port-class** [**asic** *number*] | (Optional) Display QoS port class tables.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **port-config** *port-number [asic number*] | (Optional) Display QoS port configuration information. The keywords have these meanings:<br>• *port-numbe*r—Display QoS configuration for the specified port number. The range is 0 to 25.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **port-info** *port-numbe**r*** [**asic** *number*] | (Optional) Display QoS port information. The keywords have these meanings:<br>• *port-numbe*r—Display QoS configuration for the specified port number. The range is 0 to 25.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **table-map** *table-map-name* [**asic** *number*] | (Optional) Display QoS information for the specified table map.<br>• **asic** *number*—(Optional) Display information based on the port ASIC number. The number is always 0. |
| **vlan** *vlan-id* | (Optional) Display QoS information for the specified VLAN. The range is 1 to 4094. |
| **statistics** | Display QoS interface statistics. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Command Modes** Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform resource-manager

Use the **show platform resource-manager** privileged EXEC command to display platform-dependent resource-manager information.

**show platform resource-manager** {**dm** [**index** *number*] | **erd** [**index** *number*] | **mad** [**index** *number*] | **med** [**index** *number*] | **mod** | **msm** {**hash-table [vlan** *vlan-id*] | **mac-address** *mac-address* **[vlan** *vlan-id*]**}** | **sd** [**index** *number*] | **vld** [**index** *number*]} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **dm** [**index** *number*] | Display the destination map. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **erd** [**index** *number*] | Display the equal-cost-route descriptor table for the specified index. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **mad** [**index** *number*] | Display the MAC-address descriptor table for the specified index. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **med** [**index** *number*] | Display the multi-expansion descriptor table for the specified index. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **mod** | Display the resource-manager module information. |
| **msm** {**hash-table [vlan** *vlan-id*] \| **mac-address** *mac-address* **[vlan** *vlan-id*]**}** | Display the MAC-address station descriptor table. The keywords have these meanings:<br>• **hash-table**—Display the msm hash table.<br>• **mac-address** *mac-address*—Display the table for the specified MAC address.<br>• **vlan** *vlan-id*—(Optional) Display the table for the specified VLAN. The range is 1 to 4094. |
| **sd** [**index** *number*] | Display the station descriptor table for the specified index. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **vld** [**index** *number*] | Display the VLAN-list descriptor table for the specified index. The keyword has this meaning:<br>• **index** *number*—(Optional) Display the specified index. The range is 0 to 65535. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |

| | |
|---|---|
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform snmp counters

Use the **show platform snmp counters** privileged EXEC command to display platform-dependent Simple Network Management Protocol (SNMP) counter information.

**show platform snmp counters** [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform spanning-tree synchronization

Use the **show platform spanning-tree synchronization** privileged EXEC command to display platform-dependent spanning-tree state synchronization information.

**show platform spanning-tree synchronization** [**detail | vlan** *vlan-id*] [ | {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| **detail** | (Optional) Display detailed spanning-tree synchronization information. |
| **vlan** *vlan-id* | (Optional) Display spanning-tree synchronization information for the specified VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform stp-instance

Use the **show platform stp-instance** privileged EXEC command to display platform-dependent spanning-tree instance information.

**show platform stp-instance** *vlan-id* [ **|** {**begin | exclude | include**} *expression*]

## Syntax Description

| | |
|---|---|
| *vlan-id* | Display spanning-tree instance information for the specified VLAN. The range is 1 to 4094. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform tcam

Use the **show platform tcam** privileged EXEC command to display platform-dependent ternary content addressable memory (TCAM) driver information.

**show platform tcam** {**handle** *number* | **log-results** | **table** {**acl** | **all** | **local** | **mac-address** | **qos** | **station** | **vlan-list**} | **usage**} [**asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table acl [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table all [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table local [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table mac-address [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table qos [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table station [asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**show platform tcam table vlan-list [[asic** *number* [**detail** [**invalid**]] | [**index** *number* [**detail** [**invalid**]] | **invalid** | **num** *number* [**detail** [**invalid**]] | **invalid**] | [**invalid**] | [**num** *number* [**detail** [**invalid**]] | **invalid**]] [ | {**begin** | **exclude** | **include**} *expression*]

**Syntax Description**

| | |
|---|---|
| **handle** *number* | Display the TCAM handle. The range is 0 to 4294967295. |
| **log-results** | Display the TCAM log results. |
| **table** {**acl** \| **all** \| **local** \| **mac-address** \|**qos** \| **station** \| **vlan-list**} | Display lookup and forwarding table information. The keywords have these meanings:<br>• **acl**—Display the access-control list (ACL) table.<br>• **all**—Display all the TCAM tables.<br>• **local**—Display the local table.<br>• **mac-address**—Display the MAC-address table.<br>• **qos**—Display the QoS table.<br>• **station**—Display the station table.<br>• **vlan-list**—Display the VLAN list table. |
| **usage** | Display the CAM and forwarding table usage. |
| [[**asic** *number* [**detail** [**invalid**]] \| [**index** *number* [**detail** [**invalid**]] \| **invalid** \| **num** *number* [**detail** [**invalid**]] \| **invalid**] \| [**invalid**] \| [**num** *number* [**detail** [**invalid**]] \| **invalid**]] | Display information. The keywords have these meanings:<br>• **asic** *number*—Display information for the specified ASIC device ID. The range is 0 to 15.<br>• **detail** [**invalid**]—(Optional) Display valid or invalid details.<br>• **index** *number*—(Optional) Display information for the specified TCAM table index. The range is 0 to 32768.<br>• **num** *number*—(Optional) Display information for the specified TCAM table number. The range is 0 to 32768. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **ipv6**, **equal-cost-route**, **multicast-expansion**, **secondary,** and **usage** keywords are not supported.

**Command Modes**

Privileged EXEC

**Command History**

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

**Usage Guidelines**

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# show platform vlan

Use the **show platform vlan** privileged EXEC command to display platform-dependent VLAN information.

**show platform vlan** {**misc** | **mvid** | **refcount** | **rpc** {**receive** | **transmit**}} [ | {**begin** | **exclude** | **include**} *expression*]

## Syntax Description

| | |
|---|---|
| **misc** | Display miscellaneous VLAN module information. |
| **mvid** | Display the mapped VLAN ID (MVID) allocation information. |
| **refcount** | Display the VLAN lock module-wise reference counts. |
| **rpc** {**receive** \| **transmit**} | Display remote procedure call (RPC) messages. The keywords have these meanings:<br>• **receive**—Display received information.<br>• **transmit**—Display sent information. |
| **\| begin** | (Optional) Display begins with the line that matches the *expression*. |
| **\| exclude** | (Optional) Display excludes lines that match the *expression*. |
| **\| include** | (Optional) Display includes lines that match the specified *expression*. |
| *expression* | Expression in the output to use as a reference point. |

**Note** Though visible in the command-line help strings, the **prune** keyword is not supported.

## Command Modes

Privileged EXEC

## Command History

| Release | Modification |
|---|---|
| 12.2(25)EX | This command was introduced. |

## Usage Guidelines

You should use this command only when you are working directly with your technical support representative while troubleshooting a problem. Do not use this command unless your technical support representative asks you to do so.

Expressions are case sensitive. For example, if you enter **| exclude output**, the lines that contain *output* do not appear, but the lines that contain *Output* appear.

# INDEX

## A


aaa accounting dot1x command 2-1
aaa authentication dot1x command 2-3
AAA methods 2-3
access control entries
  See ACEs
access control lists
  See ACLs
access groups
  IP 2-89
  MAC, displaying 2-309
  matching for QoS classification 2-159
access mode 2-452
access ports 2-452
ACEs 2-55, 2-186
ACLs
  as match criteria for QoS classes 2-159
  deny 2-53
  displaying 2-237
  for non-IP protocols 2-141
  IP 2-89
  on Layer 2 interfaces 2-89
  permit 2-184
action command 2-5
address aliasing 2-175
aggregate policers
  applying 2-191
  creating 2-193
  displaying 2-341
  QoS 2-194
aggregate-port learner 2-180
allowed VLANs 2-467
archive download-sw command 2-7
archive tar command 2-10
archive upload-sw command 2-13
attaching policy maps to interfaces 2-220
audience xv
authorization state of controlled port 2-61
autonegotiation of duplex mode 2-71


## B


bandwidth, configuring for QoS 2-15
bandwidth command 2-15
boot (boot loader) command A-2
boot boothlpr command 2-18
boot config-file command 2-19
boot enable-break command 2-20
boot helper command 2-21
boot helper-config file command 2-22
booting
  Cisco IOS image 2-25
  displaying environment variables 2-241
  interrupting 2-20
  manually 2-23
boot loader
  accessing A-1
  booting
    Cisco IOS image A-2
    helper image 2-21
  directories
    creating A-14
    displaying a list of A-7
    removing A-18

**boot loader (continued)**
displaying
available commands A-12
memory heap utilization A-13
version A-25
environment variables
described A-19
displaying settings A-19
location of A-20
setting A-19
unsetting A-23
files
copying A-5
deleting A-6
displaying a list of A-7
displaying the contents of A-4, A-15, A-22
renaming A-16
file system
formatting A-10
initializing flash A-9
running a consistency check A-11
prompt A-1
resetting the system A-17
boot manual command 2-23
boot private-config-file command 2-24
boot system command 2-25
BPDU filtering, for spanning tree 2-394, 2-432
BPDU guard, for spanning tree 2-396, 2-432
broadcast storm control 2-442
burst bytes, in QoS policers 2-187, 2-193

## C

cat (boot loader) command A-4
caution, description xvi
CBWFQ, configuring 2-15
channel-group command 2-26
channel-protocol command 2-30
child policy maps 2-222
class-based traffic shaping 2-235
class-based weighted fair queuing
See CBWFQ
class command 2-32
class-map command 2-34
class-map configuration mode 2-35
class maps
creating 2-34
defining the match criteria 2-160
displaying 2-245
matching in 2-34
class of service
See CoS
clear lacp command 2-38
clear mac address-table command 2-39
clear pagp command 2-40
clear policer cpu uni-eni counters command 2-41
clear port-security command 2-42
clear spanning-tree counters command 2-44
clear spanning-tree detected-protocols command 2-45
clear vmps statistics command 2-47
command modes defined 1-1
committed information rate in QoS policers 2-187, 2-193
configuration, initial
See also getting started guide and hardware installation guide
configuration files
password recovery disable considerations A-1
specifying the name 2-19, 2-24
configuring multiple interfaces 2-85
conform-action command 2-48
control-plane policer 2-41
control-plane policer information, displaying 2-342
control-plane security 2-196
control plane statistics, clearing 2-41

conventions
command xvi
for examples xvi
publication xvi
text xvi
copy (boot loader) command A-5
CoS
as match criteria for QoS groups 2-160
for QoS classification 2-224
setting value in policy maps 2-224
CPU ASIC statistics, displaying 2-246
CPU protection policers, displaying C-16

## D

debug dot1x command B-2
debug etherchannel command B-3
debug interface command B-4
debug ip igmp filter command B-5
debug ip igmp max-groups command B-6
debug ip igmp snooping command B-7
debug lacp command B-8
debug mac-notification command B-9
debug matm command B-10
debug monitor command B-11
debug mvrdbg command B-12
debug nvram command B-13
debug pagp command B-14
debug platform acl command B-15
debug platform cpu-queues command B-16
debug platform dot1x command B-18
debug platform etherchannel command B-19
debug platform forw-tcam command B-20
debug platform ip dhcp command B-21
debug platform ip igmp snooping command B-22
debug platform led command B-24
debug platform matm command B-25
debug platform messaging application command B-26
debug platform phy command B-27
debug platform pm command B-29
debug platform policer cpu uni-eni command B-31
debug platform port-asic command B-32
debug platform port-security command B-33
debug platform qos-acl-tcam command B-34
debug platform remote-commands command B-35
debug platform resource-manager command B-36
debug platform snmp command B-37
debug platform span command B-38
debug platform supervisor-asic command B-39
debug platform sw-bridge command B-40
debug platform tcam command B-41
debug platform udld command B-43
debug platform vlan command B-44
debug pm command B-45
debug port-security command B-47
debug qos-manager command B-48
debug spanning-tree bpdu command B-51
debug spanning-tree bpdu-opt command B-52
debug spanning-tree command B-49
debug spanning-tree mstp command B-53
debug spanning-tree switch command B-55
debug sw-vlan command B-57
debug sw-vlan ifs command B-58
debug sw-vlan notification command B-59
debug udld command B-61
debug vqpc command B-63
default
policer configuration
NNIs C-18
UNIs C-17
define interface-range command 2-50
delete (boot loader) command A-6
delete command 2-52
deny command 2-53

detect mechanism, causes 2-72
DHCP snooping
accepting untrusted packets from edge switch 2-100
enabling
on a VLAN 2-106
option 82 2-98, 2-100
trust on an interface 2-104
error recovery timer 2-77
rate limiting 2-103
DHCP snooping binding database
binding file, configuring 2-96
bindings
adding 2-94
deleting 2-94
displaying 2-289
clearing database agent statistics 2-36
database agent, configuring 2-96
displaying
binding entries 2-289
database agent status 2-291, 2-293
renewing 2-215
differentiated service code point
See DSCP
dir (boot loader) command A-7
directories, deleting 2-52
documentation, related xvi
document conventions xvi
dot1x default command 2-56
dot1x host-mode command 2-57
dot1x initialize command 2-58
dot1x max-req command 2-59, 2-60
dot1x port-control command 2-61
dot1x re-authenticate command 2-63
dot1x reauthentication command 2-64
dot1x system-auth-control command 2-65
dot1x test eapol-capable command 2-66
dot1x test timeout command 2-67
dot1x timeout command 2-68
dropping packets, with ACL matches 2-5
DSCP
as match criteria for QoS groups 2-161
for QoS traffic marking 2-226
setting in policy maps 2-226
duplex command 2-70
dynamic-access ports
configuring 2-447
restrictions 2-448
Dynamic Host Configuration Protocol (DHCP)
See DHCP snooping

## E

EAP-request/identity frame
maximum number to send 2-60
response time before retransmitting 2-68
environment variables, displaying 2-241
errdisable detect cause command 2-72
errdisable detect cause small-frame comand 2-74
errdisable recovery cause small-frame 2-76
errdisable recovery command 2-77
error conditions, displaying 2-265
error disable detection 2-72
error-disabled interfaces, displaying 2-276
EtherChannel
assigning Ethernet interface to channel group 2-26
creating port-channel logical interface 2-83
debug EtherChannel/PAgP, display B-3
debug platform-specific events, display B-19
displaying 2-269
interface information, displaying 2-276
LACP
clearing channel-group information 2-38
debug messages, display B-8
displaying 2-305
modes 2-26
port priority for hot-standby ports 2-132
restricting a protocol 2-30
system priority 2-134

**EtherChannel (continued)**
load-distribution methods 2-200
PAgP
aggregate-port learner 2-180
clearing channel-group information 2-40
debug messages, display B-14
displaying 2-337
error detection for 2-72
error recovery timer 2-77
learn method 2-180
modes 2-26
physical-port learner 2-180
priority of interface for transmitted traffic 2-182
Ethernet controller, internal register display 2-248
Ethernet statistics, collecting 2-217
examples, conventions for xvi
exceed-action command 2-79
extended-range VLANs
and allowed VLAN list 2-467
configuring 2-486
extended system ID for STP 2-402

## F

fan information, displaying 2-262
files, deleting 2-52
flash_init (boot loader) command A-9
flowcontrol command 2-81
format (boot loader) command A-10
forwarding packets, with ACL matches 2-5
forwarding results, display C-5
frame forwarding information, displaying C-5
fsck (boot loader) command A-11

## G

global configuration mode 1-2, 1-3

## H

hardware ACL statistics 2-237
help (boot loader) command A-12
host connection, port configuration 2-451
host ports, private VLANs 2-454

## I

IEEE 802.1x
and switchport modes 2-453
violation error recovery 2-77
See also port-based authentication
IGMP filters
applying 2-109
debug messages, display B-5
IGMP groups, setting maximum 2-111
IGMP maximum groups, debugging B-6
IGMP profiles
creating 2-113
displaying 2-296
IGMP snooping
adding ports as a static member of a group 2-128
displaying 2-297, 2-301, 2-303
enabling 2-115
enabling the configurable-leave timer 2-117
enabling the Immediate-Leave feature 2-125
flooding query count 2-123
interface topology change notification behavior 2-124
multicast table 2-299
querier 2-119
query solicitation 2-123
report suppression 2-121
switch topology change notification behavior 2-123
images
See software images
Immediate-Leave feature, MVR 2-177
immediate-leave processing 2-125

initial configuration
See also getting started guide and hardware installation guide
input policy maps
and ACL classification 2-159
and aggregate policers 2-194
commands not supported in 2-198
configuration guidelines 2-198
interface command 2-88
interface configuration mode 1-2, 1-4
interface port-channel command 2-83
interface range command 2-85
interface-range macros 2-50
interfaces
assigning Ethernet interface to channel group 2-26
configuring 2-70
configuring multiple 2-85
creating port-channel logical 2-83
debug messages, display B-4
disabling 2-379
displaying the MAC address table 2-321
restarting 2-379
interface speed, configuring 2-440
internal registers, displaying 2-248, 2-255
Internet Group Management Protocol
See IGMP
invalid GBIC
error detection for 2-72
error recovery timer 2-77
ip address command 2-91
IP addresses, setting 2-91
IP address matching 2-157
IP DHCP snooping
See DHCP snooping
ip dhcp snooping binding command 2-94
ip dhcp snooping command 2-93
ip dhcp snooping database command 2-96
ip dhcp snooping information option allow-untrusted command 2-100
ip dhcp snooping information option command 2-98
ip dhcp snooping information option format remote-id command 2-102
ip dhcp snooping limit rate command 2-103
ip dhcp snooping trust command 2-104
ip dhcp snooping verify command 2-105
ip dhcp snooping vlan command 2-106
ip dhcp snooping vlan information option format-type circuit-id string command 2-107
ip igmp filter command 2-109
ip igmp max-groups command 2-111
ip igmp profile command 2-113
ip igmp snooping command 2-115
ip igmp snooping last-member-query-interval command 2-117
ip igmp snooping querier command 2-119
ip igmp snooping report-suppression command 2-121
ip igmp snooping tcn command 2-123
ip igmp snooping tcn flood command 2-124
ip igmp snooping vlan immediate-leave command 2-125
ip igmp snooping vlan mrouter command 2-126
ip igmp snooping vlan static command 2-128
IP multicast addresses 2-174
IP precedence, as match criteria for QoS groups 2-163
IP source guard, displaying dynamic binding entries 2-289
ip ssh command 2-130

## J

jumbo frames
See MTU

## L

LACP
See EtherChannel
lacp port-priority command 2-132
lacp system-priority command 2-134

Layer 2 traceroute
IP addresses 2-477
MAC addresses 2-474
line configuration mode 1-2, 1-4
Link Aggregation Control Protocol
See EtherChannel
link flap
error detection for 2-72
error recovery timer 2-77
load-distribution methods for EtherChannel 2-200
logging event command 2-136
logging file command 2-137
logical interface 2-83
loopback error
detection for 2-72
recovery timer 2-77
loop guard, for spanning tree 2-404, 2-408

## M

mac access-group command 2-139
MAC access-groups, displaying 2-309
MAC access list configuration mode 2-141
mac access-list extended command 2-141
MAC access lists 2-53
MAC addresses
displaying
aging time 2-315
all 2-313
dynamic 2-319
notification settings 2-323
number of addresses in a VLAN 2-317
per interface 2-321
per VLAN 2-327
static 2-325
static and dynamic entries 2-311
MAC addresses (continued)
dynamic
aging time 2-143
deleting 2-39
displaying 2-319
enabling MAC address notification 2-144
matching 2-157
static
adding and removing 2-146
displaying 2-325
dropping on an interface 2-147
tables 2-313
MAC address notification, debugging B-9
mac address-table aging-time 2-139, 2-157
mac address-table aging-time command 2-143
mac address-table notification command 2-144
mac address-table static command 2-146
mac address-table static drop command 2-147
macro description command 2-151
macro global command 2-152
macro global description command 2-154
macro name command 2-155
macros
adding a description 2-151
adding a global description 2-154
applying 2-152
creating 2-155
displaying 2-339
interface range 2-50, 2-85
specifying parameter values 2-152
tracing 2-152
manual
audience xv
purpose of xv
mapping tables, QoS 2-471

maps
class
creating 2-34
VLAN
creating 2-489
defining 2-157
displaying 2-374
match access-group command 2-159
match cos command 2-160
match ip dscp command 2-161
match ip precedence command 2-163
match qos-group command 2-165
maximum transmission unit
See MTU
mdix auto command 2-167
memory (boot loader) command A-13
mkdir (boot loader) command A-14
mode, MVR 2-174
modes, commands 1-1
monitor session command 2-169
more (boot loader) command A-15
MSTP
displaying 2-355
interoperability 2-45
link type 2-406
MST region
aborting changes 2-412
applying changes 2-412
configuration name 2-412
configuration revision number 2-413
current or pending display 2-413
displaying 2-355
MST configuration mode 2-412
VLANs-to-instance mapping 2-412
path cost 2-414
protocol mode 2-410
restart protocol migration process 2-45

MSTP (continued)
root port
loop guard 2-404
preventing from becoming designated 2-404
restricting which can be root 2-404
root guard 2-404
root switch
affects of extended system ID 2-402
hello-time 2-417, 2-428
interval between BDPU messages 2-419
interval between hello BPDU messages 2-417, 2-428
max-age 2-419
maximum hop count before discarding BPDU 2-421
port priority for selection of 2-423
primary or secondary 2-428
switch priority 2-426
state changes
blocking to forwarding state 2-435
enabling BPDU filtering 2-394, 2-432
enabling BPDU guard 2-396, 2-432
enabling Port Fast 2-432, 2-435
forward-delay time 2-416
length of listening and learning states 2-416
rapid transition to forwarding 2-406
shutting down Port Fast-enabled ports 2-432
state information display 2-354
MTU
configuring size 2-469
displaying global setting 2-362
multicast group address, MVR 2-177
multicast groups, MVR 2-175
multicast router learning method 2-126
multicast router ports, configuring 2-126
multicast storm control 2-442
multicast VLAN, MVR 2-174
multicast VLAN registration
See MVR

multiple hosts on authorized port 2-57
Multiple Spanning Tree Protocol
See MSTP
MVR
and address aliasing 2-175
configuring 2-174
configuring interfaces 2-177
debug messages, display B-12
displaying 2-331
displaying interface information 2-333
members, displaying 2-335
mvr (global configuration) command 2-174
mvr (interface configuration) command 2-177
mvr vlan group command 2-178

## N

native VLANs 2-467
network node interface 2-202
nonegotiate, speed 2-440, 2-441
non-IP protocols
denying 2-53
forwarding 2-184
non-IP traffic access lists 2-141
non-IP traffic forwarding
denying 2-53
permitting 2-184
normal-range VLANs 2-486
note, description xvi
no vlan command 2-486

## O

output policy maps
and QoS group classification 2-165
and traffic shaping 2-235
commands not supported in 2-198
configuration guidelines 2-198
**output policy maps (continued)**
priority in 2-205
queue limit in 2-210

## P

PAgP
See EtherChannel
pagp learn-method command 2-180
pagp port-priority command 2-182
parent policy maps 2-222
password-recovery mechanism, enabling and disabling 2-218
permit command 2-184
per-VLAN spanning-tree plus
See STP
physical-port learner 2-180
PID, displaying 2-286
PIM-DVMRP, as multicast router learning method 2-126
police
multiple conform actions for a class 2-48
multiple exceed actions for a class 2-79
with priority 2-187
police aggregate command 2-191
police command 2-187
policer aggregate command 2-193
policer configuration
default for NNIs C-18
default for UNIs C-17
policer cpu uni command 2-196
policers
aggregate 2-191, 2-193
for CPU protection 2-196
individual 2-187
policy-map class, configuring multiple actions 2-48, 2-79
policy-map class configuration mode 2-32
policy-map class police configuration mode 2-48, 2-189
policy-map command 2-197
policy-map configuration mode 2-197

policy maps
and CoS classification 2-160
and DSCP classification 2-161
and IP precedence classification 2-163
and policing 2-189
applying 2-220
applying to an interface 2-198, 2-220, 2-232
child 2-222
creating 2-197
displaying 2-344
hierarchical 2-222
parent 2-222
policers
for a single class 2-187
for multiple classes 2-191, 2-193, 2-196, 2-222
setting priority 2-204
setting QoS group identifier 2-230
traffic classification, defining 2-32
traffic marking
setting CoS values 2-224
setting DSCP values 2-226
setting IP precedence values 2-228
Port Aggregation Protocol
See EtherChannel
port-based authentication
AAA method list 2-3
debug messages, display B-2
enabling 802.1x
globally 2-65
per interface 2-61
host modes 2-57
IEEE 802.1x AAA accounting methods 2-1
initialize an interface 2-58, 2-67
manual control of authorization state 2-61
multiple hosts on authorized port 2-57
periodic re-authentication
enabling 2-64
time between attempts 2-68
**port-based authentication (continued)**
quiet period between failed authentication exchanges 2-68
re-authenticating 802.1x-enabled ports 2-63
resetting configurable 802.1x parameters 2-56
switch-to-authentication server retransmission time 2-68
switch-to-client frame-retransmission number 2-59 to 2-60
switch-to-client retransmission time 2-68
test for IEEE 802.1x readiness 2-66
port-channel load-balance command 2-200
Port Fast, for spanning tree 2-435
port ranges, defining 2-50
ports, debugging B-45
ports, protected 2-465
port security
aging 2-461
debug messages, display B-47
enabling 2-457
violation error recovery 2-77
port shaping 2-236
port-type command 2-202
port types, MVR 2-177
power information, displaying 2-262
precedence
for QoS traffic marking 2-228
setting in policy maps 2-228
priority command 2-204
priority queuing, QoS 2-204
priority with police, QoS 2-204
private-vlan command 2-207
private VLANs
association 2-463
configuring 2-207
configuring ports 2-454
displaying 2-369
host ports 2-454

**private VLANs (continued)**
mapping
configuring 2-463
promiscuous ports 2-454
privileged EXEC mode 1-2, 1-3
product identification information, displaying 2-286
promiscuous ports, private VLANs 2-454
PVST+
See STP

## Q

QoS
aggregate policers
applying 2-191
creating 2-193
displaying 2-341
class maps
creating 2-34
defining the match criteria 2-160
displaying 2-245
displaying statistics for 2-344, C-24
policy maps
applying an aggregate policer 2-191, 2-193, 2-196, 2-222
applying to an interface 2-220, 2-232
creating 2-197
defining policers 2-187
displaying policy maps 2-344
setting CoS values 2-224
setting DSCP values 2-226
setting IP precedence values 2-228
setting QoS group identifier 2-230
traffic classifications 2-32
table maps
configuring 2-471
displaying 2-363
QoS groups
as match criteria 2-165
for QoS traffic classification 2-230
setting in policy maps 2-230
QoS match criteria
ACLs 2-159
CoS value 2-160
DSCP value 2-161
precedence value 2-163
QoS group number 2-165
quality of service
See QoS
querytime, MVR 2-174
queue-limit command 2-210

## R

rapid per-VLAN spanning-tree plus
See STP
rapid PVST+
See STP
re-authenticating 802.1x-enabled ports 2-63
re-authentication
periodic 2-64
time between attempts 2-68
receiver ports, MVR 2-177
receiving flow-control packets 2-81
recovery mechanism
causes 2-77
display 2-243, 2-263, 2-267
timer interval 2-77
remote-span command 2-213
Remote Switched Port Analyzer
See RSPAN
rename (boot loader) command A-16
renew ip dhcp snooping database command 2-215
reset (boot loader) command A-17
rmdir (boot loader) command A-18
rmon collection stats command 2-217

root guard, for spanning tree 2-404
RSPAN
configuring 2-169
displaying 2-329
filter RSPAN traffic 2-169
remote-span command 2-213
sessions
add interfaces to 2-169
displaying 2-329
start new 2-169

## S

SDM templates
displaying 2-353
secure ports, limitations 2-459
sending flow-control packets 2-81
service password-recovery command 2-218
service policy (policy-map class configuration) command 2-222
service-policy interface configuration command 2-220
service-policy policy-map class configuration command 2-222
set (boot loader) command A-19
set cos command 2-224
set dscp command 2-226
set precedence command 2-228
set qos-group command 2-230
setup command 2-232
SFPs, displaying information about 2-286
shape average command 2-235
show access-lists command 2-237
show aggregate-policer command 2-363
show archive status command 2-240
show boot command 2-241
show class-map command 2-245
show controllers cpu-interface command 2-246
show controllers ethernet-controller command 2-248
show controllers tcam command 2-255
show controllers utilization command 2-257
show controller utilization command 2-257
show dot1x command 2-259
show env command 2-262
show errdisable detect command 2-263
show errdisable flap-values command 2-265
show errdisable recovery command 2-267
show etherchannel command 2-269
show flowcontrol command 2-272
show idprom command 2-274
show interfaces command 2-276
show interfaces counters command 2-284
show inventory command 2-286
show ip dhcp snooping binding command 2-289
show ip dhcp snooping command 2-288
show ip dhcp snooping database command 2-291, 2-293
show ip igmp profile command 2-296
show ip igmp snooping command 2-297
show ip igmp snooping command querier detail 2-303
show ip igmp snooping groups command 2-299
show ip igmp snooping mrouter command 2-301
show ip igmp snooping querier command 2-303
show ip igmp snooping querier detail command 2-303
show lacp command 2-305
show location 2-309
show mac access-group command 2-309
show mac address-table address command 2-313
show mac address-table aging time command 2-315
show mac address-table command 2-311
show mac address-table count command 2-317
show mac address-table dynamic command 2-319
show mac address-table interface command 2-321
show mac address-table notification command 2-323
show mac address-table static command 2-325
show mac address-table vlan command 2-327
show monitor command 2-329
show mvr command 2-331
show mvr interface command 2-333
show mvr members command 2-335

show pagp command 2-337
show parser macro command 2-339
show platform acl command C-2
show platform configuration command C-3
show platform etherchannel command C-4
show platform forward command C-5
show platform igmp snooping command C-7
show platform layer4op command C-9
show platform mac-address-table command C-10
show platform messaging command C-11
show platform monitor command C-12
show platform mvr table command C-13
show platform pm command C-14
show platform policer cpu command C-16
show platform port-asic command C-19
show platform port-security command C-23
show platform qos command C-24
show platform resource-manager command C-27
show platform snmp counters command C-29
show platform spanning-tree synchronization command C-30
show platform stp-instance command C-31
show platform tcam command C-32
show platform vlan command C-35
show policer aggregate command 2-341
show policer cpu uni-eni command 2-342
show policy-map command 2-344
show policy-map interface output fields 2-347
show port security command 2-348
show port-type command 2-351
show sdm prefer command 2-353
show spanning-tree command 2-354
show storm-control command 2-360
show system mtu command 2-362
show udld command 2-365
show version command 2-367
show vlan access-map command 2-374
show vlan command 2-369
show vlan command, fields 2-371
show vlan filter command 2-375
show vmps command 2-377
shutdown command 2-379
shutdown vlan command 2-380
small violation-rate command 2-381
SNMP host, specifying 2-386
SNMP informs, enabling the sending of 2-383
snmp-server enable traps command 2-383
snmp-server host command 2-386
snmp trap mac-notification command 2-390
SNMP traps
  enabling MAC address notification trap 2-390
  enabling the MAC address notification feature 2-144
  enabling the sending of 2-383
software images
  deleting 2-52
  downloading 2-7
  upgrading 2-7
  uploading 2-13
software version, displaying 2-367
source ports, MVR 2-177
SPAN
  configuring 2-169
  debug messages, display B-11
  displaying 2-329
  filter SPAN traffic 2-169
  sessions
    add interfaces to 2-169
    displaying 2-329
    start new 2-169
spanning-tree bpdufilter command 2-392, 2-394
spanning-tree bpduguard command 2-396
spanning-tree cost command 2-398
spanning-tree etherchannel command 2-400
spanning-tree extend system-id command 2-402
spanning-tree guard command 2-404
spanning-tree link-type command 2-406
spanning-tree loopguard default command 2-408
spanning-tree mode command 2-410

spanning-tree mst configuration command 2-412
spanning-tree mst cost command 2-414
spanning-tree mst forward-time command 2-416
spanning-tree mst hello-time command 2-417
spanning-tree mst max-age command 2-419
spanning-tree mst max-hops command 2-421
spanning-tree mst port-priority command 2-423
spanning-tree mst pre-standard command 2-425
spanning-tree mst priority command 2-426
spanning-tree mst root command 2-428
spanning-tree portfast (global configuration) command 2-432
spanning-tree portfast (interface configuration) command 2-435
spanning-tree port-priority command 2-430
Spanning Tree Protocol
  See STP
spanning-tree vlan command 2-437
speed command 2-440
SSH, configuring version 2-130
static-access ports, configuring 2-447
statistics, Ethernet group 2-217
sticky learning, enabling 2-457
storm-control command 2-442
STP
  counters, clearing 2-44
  debug messages, display
    MSTP B-53
    optimized BPDUs handling B-52
    spanning-tree activity B-49
    switch shim B-55
    transmitted and received BPDUs B-51
  enabling on ENIs 2-392
  EtherChannel misconfiguration 2-400
  extended system ID 2-402
  path cost 2-398
  protocol modes 2-410

**STP (continued)**
  root port
    loop guard 2-404
    preventing from becoming designated 2-404
    restricting which can be root 2-404
    root guard 2-404
  root switch
    affects of extended system ID 2-402, 2-438
    hello-time 2-437
    interval between BDPU messages 2-437
    interval between hello BPDU messages 2-437
    max-age 2-437
    port priority for selection of 2-430
    primary or secondary 2-437
    switch priority 2-437
  state changes
    blocking to forwarding state 2-435
    enabling BPDU filtering 2-394, 2-432
    enabling BPDU guard 2-396, 2-432
    enabling Port Fast 2-432, 2-435
    enabling timer to recover from error state 2-77
    forward-delay time 2-437
    length of listening and learning states 2-437
    shutting down Port Fast-enabled ports 2-432
  state information display 2-354
  VLAN options 2-426, 2-437
Switched Port Analyzer
  See SPAN
switching characteristics
  modifying 2-445
  returning to interfaces 2-445
switchport access command 2-447
switchport block command 2-449
switchport command 2-445
switchport host command 2-451
switchport mode command 2-452
switchport mode private-vlan command 2-454

switchport port-security aging command 2-461
switchport port-security command 2-457
switchport private-vlan command 2-463
switchport protected command 2-465
switchports, displaying 2-276
switchport trunk command 2-467
system message logging, save message to flash 2-137
system mtu command 2-469

## T

table-map command 2-471
table-map configuration mode 2-471
table maps
  configuring 2-471
  displaying 2-363
  QoS 2-471
tar files, creating, listing, and extracting 2-10
TDR, running 2-473
temperature information, displaying 2-262
test cable-diagnostics tdr command 2-473
traceroute mac command 2-474
traceroute mac ip command 2-477
traffic shaping, QoS 2-235
trunking, VLAN mode 2-452
trunk mode 2-452
trunk ports 2-452
type (boot loader) command A-22

## U

UDLD
  aggressive mode 2-479, 2-481
  debug messages, display B-61
  enable globally 2-479
  enable per interface 2-481
  error recovery timer 2-77
  message timer 2-479

**UDLD (continued)**

  normal mode 2-479, 2-481
  reset a shutdown interface 2-483
  status 2-365
udld command 2-479
udld port command 2-481
udld reset command 2-483
unicast storm control 2-442
UniDirectional Link Detection
  See UDLD
uni-vlan command 2-484
unknown multicast traffic, preventing 2-449
unknown unicast traffic, preventing 2-449
unset (boot loader) command A-23
upgrading
  software images 2-7
    monitoring status of 2-240
upgrading information
  See release notes
user EXEC mode 1-2
user network interface 2-202

## V

version (boot loader) command A-25
vlan access-map command 2-489
VLAN access map configuration mode 2-489
VLAN access maps
  actions 2-5
  displaying 2-374
vlan command 2-486
VLAN configuration mode
  commands 2-486
  description 1-4
  entering 2-486
  summary 1-2
vlan filter command 2-491

VLAN filters, displaying 2-375
VLAN ID range 2-486
VLAN maps
  applying 2-491
  creating 2-489
  defining 2-157
  displaying 2-374
VLAN Query Protocol
  See VQP
VLANs
  adding 2-486
  configuring 2-486
  debug messages, display
    activation of B-59
    VLAN IOS file system error tests B-58
    VLAN manager activity B-57
  displaying configurations 2-369
  extended-range 2-486
  MAC addresses
    displaying 2-327
    number of 2-317
  normal-range 2-486
  private 2-454
    configuring 2-207
    displaying 2-369
    See also private VLANs
  restarting 2-380
  saving the configuration 2-486
  shutting down 2-380
  suspending 2-380
VMPS
  configuring servers 2-496
  displaying 2-377
  error recovery timer 2-77
  reconfirming dynamic VLAN assignments 2-493
vmps reconfirm (global configuration) command 2-494
vmps reconfirm (privileged EXEC) command 2-493
vmps retry command 2-495
vmps server command 2-496
VQP
  and dynamic-access ports 2-448
  clearing client statistics 2-47
  displaying information 2-377
  per-server retry count 2-495
  reconfirmation interval 2-494
  reconfirming dynamic VLAN assignments 2-493

## W

Weighted Tail Drop
  See WTD
WTD, queue-limit command 2-210